НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2026-06-10.1 | 10 июня 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-35205	РЕД ОС	Локальный	OSI	2026-05-20	✓
2	Высокая	CVE-2026-35204	РЕД ОС	Локальный	OSI	2026-05-21	✓
3	Высокая	CVE-2026-32241	РЕД ОС	Сетевой	ACE	2026-05-18	✓
4	Высокая	CVE-2026-27623	РЕД ОС	Сетевой	DoS	2026-05-18	✓
5	Высокая	CVE-2026-31899	РЕД ОС	Сетевой	DoS	2026-05-18	✓
6	Критическая	CVE-2026-6366	Drupal	Сетевой	ACE	2026-04-23	✓
7	Высокая	CVE-2026-33898	РЕД ОС	Сетевой	PE	2026-05-21	✓
8	Высокая	CVE-2026-32609	РЕД ОС	Сетевой	OSI	2026-05-25	✓
9	Высокая	CVE-2026-34930	Apex One	Локальный	PE	2026-05-26	✓
10	Высокая	CVE-2026-45207	Apex One	Локальный	PE	2026-05-26	✓
11	Высокая	CVE-2026-45208	Apex One	Локальный	PE	2026-05-26	✓
12	Высокая	CVE-2026-45206	Apex One	Локальный	PE	2026-05-26	✓
13	Высокая	CVE-2026-34929	Apex One	Локальный	PE	2026-05-26	✓

14	Высокая	CVE-2026-34927	Apex One	Локальный	PE	2026-05-26	✓
15	Высокая	CVE-2026-8092	Firefox	Сетевой	ACE	2026-05-26	✓
16	Высокая	CVE-2026-48844	RoundCube Webmail	Сетевой	ACE	2026-05-26	✓
17	Высокая	CVE-2026-48842	RoundCube Webmail	Сетевой	ACE	2026-05-26	✓
18	Высокая	CVE-2026-7320	Firefox	Сетевой	OSI	2026-05-26	✓
19	Критическая	CVE-2026-9543	N300RH	Сетевой	ACE	2026-05-28	✓
20	Высокая	CVE-2026-34928	Apex One	Локальный	PE	2026-05-26	✓
21	Высокая	CVE-2026-9431	Tenda F1202	Сетевой	ACE	2026-05-27	✓
22	Критическая	CVE-2026-0263	PAN-OS	Сетевой	ACE	2026-05-25	✓
23	Высокая	CVE-2026-9429	Tenda F1202	Сетевой	ACE	2026-05-27	✓
24	Высокая	CVE-2026-9428	Tenda F1202	Сетевой	ACE	2026-05-27	✓
25	Высокая	CVE-2026-9430	Tenda F1202	Сетевой	ACE	2026-05-27	✓
26	Критическая	CVE-2026-44930	CXF	Сетевой	OSI	2026-05-27	✓
27	Высокая	CVE-2026-27771	Gitea	Сетевой	OSI	2026-05-28	✓
28	Высокая	CVE-2026-4868	Gitlab	Сетевой	CI	2026-05-28	✓

29	Высокая	CVE-2026-7081	Tenda F456	Сетевой	ACE	2026-05-04	✓
30	Высокая	CVE-2026-7082	Tenda F456	Сетевой	ACE	2026-05-04	✓
31	Высокая	CVE-2026-5992	Tenda F451	Сетевой	ACE	2026-05-05	✓
32	Высокая	CVE-2026-2905	Tenda HG9	Сетевой	ACE	2026-05-05	✓
33	Высокая	CVE-2026-5990	Tenda F451	Сетевой	DoS	2026-05-05	✓
34	Критическая	CVE-2026-5997	A7100RU	Сетевой	ACE	2026-05-05	✓
35	Критическая	CVE-2026-5996	A7100RU	Сетевой	ACE	2026-05-05	✓
36	Критическая	CVE-2026-5995	A7100RU	Сетевой	ACE	2026-05-05	✓
37	Критическая	CVE-2026-5993	A7100RU	Сетевой	ACE	2026-05-05	✓
38	Высокая	CVE-2026-5991	Tenda F451	Сетевой	DoS	2026-05-05	✓
39	Высокая	CVE-2026-2927	DWR-M960	Сетевой	ACE	2026-05-05	✓
40	Высокая	BDU:2026-07491	Gogs	Сетевой	ACE	2026-05-29	✓
41	Критическая	CVE-2026-5994	A7100RU	Сетевой	ACE	2026-05-05	✓
42	Высокая	CVE-2026-48778	Notepad++	Локальный	ACE	2026-05-29	✓
43	Высокая	CVE-2026-48800	Notepad++	Локальный	ACE	2026-05-29	✓

44	Высокая	CVE-2026-39829	crypto	Сетевой	DoS	2026-05-27	✓
45	Высокая	CVE-2026-2910	Tenda HG9	Сетевой	ACE	2026-05-25	✓
46	Высокая	CVE-2026-2909	Tenda HG9	Сетевой	ACE	2026-05-25	✓
47	Высокая	CVE-2026-7288	DIR-825M	Сетевой	ACE	2026-05-19	✓
48	Высокая	CVE-2026-7289	DIR-825M	Сетевой	ACE	2026-05-19	✓
49	Высокая	CVE-2026-2929	DWR-M960	Сетевой	ACE	2026-05-05	✓
50	Высокая	CVE-2026-2926	DWR-M960	Сетевой	DoS	2026-05-05	✓
51	Высокая	CVE-2026-2908	Tenda HG9	Сетевой	ACE	2026-05-25	✓
52	Критическая	CVE-2026-6026	A7100RU	Сетевой	ACE	2026-04-14	✓
53	Критическая	CVE-2026-6027	A7100RU	Сетевой	ACE	2026-04-14	✓
54	Критическая	CVE-2026-6025	A7100RU	Сетевой	ACE	2026-04-14	✓
55	Высокая	CVE-2026-6157	A800R	Сетевой	DoS	2026-04-14	✓
56	Критическая	CVE-2026-6156	A7100RU	Сетевой	ACE	2026-04-14	✓
57	Критическая	CVE-2026-6028	A7100RU	Сетевой	ACE	2026-04-14	✓
58	Критическая	CVE-2026-6132	A7100RU	Сетевой	ACE	2026-04-14	✓

59	Критическая	CVE-2026-6155	A7100RU	Сетевой	ACE	2026-04-14	✓
60	Критическая	CVE-2026-6029	A7100RU	Сетевой	ACE	2026-04-14	✓
61	Критическая	CVE-2026-6154	A7100RU	Сетевой	ACE	2026-04-14	✓
62	Критическая	CVE-2026-6195	A7100RU	Сетевой	ACE	2026-04-07	✓
63	Высокая	CVE-2026-24150	Megatron-LM	Локальный	ACE	2026-03-31	✓
64	Высокая	CVE-2026-8053	MongoDB	Сетевой	ACE	2026-06-01	✓
65	Высокая	CVE-2026-4976	LR350	Сетевой	DoS	2026-04-02	✓
66	Высокая	CVE-2026-24152	Megatron-LM	Локальный	ACE	2026-03-31	✓
67	Критическая	CVE-2026-30884	moodle-mod_customcert	Сетевой	OSI	2026-03-18	✓
68	Высокая	CVE-2026-24151	Megatron-LM	Локальный	ACE	2026-03-31	✓
69	Высокая	CVE-2026-10161	TRENDnet TEW-432BRP	Сетевой	ACE	2026-06-01	✓
70	Высокая	CVE-2020-36984	CX17NF-WF	Локальный	ACE	2026-02-02	✓
71	Критическая	CVE-2026-41901	Thymeleaf	Сетевой	ACE	2026-05-27	✓
72	Высокая	CVE-2024-11954	pimcore	Сетевой	XSS\CSS	2025-02-06	✓
73	Высокая	CVE-2026-5740	Mattermost	Сетевой	DoS	2026-05-27	✓

74	Высокая	CVE-2026-5308	Mattermost	Сетевой	DoS	2026-05-27	✓
75	Критическая	CVE-2026-34177	Ubuntu	Сетевой	PE	2026-05-29	✓
76	Критическая	CVE-2026-34178	Ubuntu	Сетевой	ACE	2026-05-29	✓
77	Критическая	CVE-2026-34179	Ubuntu	Сетевой	PE	2026-05-29	✓
78	Высокая	CVE-2026-29923	PowerStrip	Локальный	PE	2026-04-21	✓
79	Критическая	CVE-2026-29014	Metinfo	Сетевой	ACE	2026-05-06	✓
80	Высокая	CVE-2026-33540	Debian GNU/Linux	Сетевой	ACE	2026-05-28	✓
81	Высокая	CVE-2026-35172	Debian GNU/Linux	Сетевой	PE	2026-05-28	✓
82	Высокая	CVE-2026-10162	TRENDnet TEW-432BRP	Сетевой	ACE	2026-06-01	✓
83	Высокая	CVE-2026-10160	TRENDnet TEW-432BRP	Сетевой	ACE	2026-06-01	✓
84	Высокая	CVE-2026-10158	TRENDnet TEW-432BRP	Сетевой	ACE	2026-06-01	✓
85	Высокая	CVE-2026-10159	TRENDnet TEW-432BRP	Сетевой	ACE	2026-06-01	✓
86	Высокая	CVE-2026-32877	botan	Сетевой	DoS	2026-04-08	✓
87	Высокая	CVE-2026-10120	TRENDnet TEW-432BRP	Сетевой	ACE	2026-06-01	✓
88	Высокая	CVE-2026-10119	TRENDnet TEW-432BRP	Сетевой	ACE	2026-06-01	✓

89	Высокая	CVE-2026-8697	Archer C64	Смежная сеть	ACE	2026-05-29	✓
90	Высокая	CVE-2026-46243	Linux	Локальный	ACE	2026-06-01	✓
91	Высокая	CVE-2026-4430	LibreOffice AgileEngine	Локальный	ACE	2026-06-01	✓
92	Критическая	CVE-2026-7858	Magic Collaboration Studio	Сетевой	ACE	2026-06-01	✓
93	Критическая	CVE-2026-45321	TanStack	Сетевой	ACE	2026-05-29	✓
94	Высокая	CVE-2026-10701	Mozilla Firefox	Сетевой	ACE	2026-06-03	✓

1

Краткое описание: Получение конфиденциальной информации в РЕД ОС

Идентификатор уязвимости: CVE-2026-35205
BDU:2026-07345

Идентификатор программной ошибки: CWE-636 Небезопасное восстановление после сбоя (сбой с открытием доступа)

Уязвимый продукт: РЕД ОС: 8.0
Helm: до 4.1.4

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-20 / 2026-05-20

Ссылки на источник:

- https://github.com/helm/helm
- https://github.com/helm/helm/commit/05fa37973dc9e42b76e1d2883494c87174b6074f
- https://github.com/helm/helm/releases/tag/v4.1.4
- https://github.com/helm/helm/security/advisories/GHSA-q5jf-9vfq-h4h7
- https://helm.sh/docs/topics/provenance/#the-provenance-file
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-35205
- https://bdu.fstec.ru/vul/2026-07345

2

Краткое описание: Получение конфиденциальной информации в РЕД ОС

Идентификатор уязвимости: CVE-2026-35204
BDU:2026-07346

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: РЕД ОС: 8.0
Helm: от 4.0.0 до 4.1.4

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.6 AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://github.com/helm/helm/security/advisories/GHSA-vmx8-mqv2-9gmg
- https://github.com/helm/helm/releases/tag/v4.1.4
- https://github.com/helm/helm
- https://github.com/helm/helm/commit/36c8539e99bc42d7aef9b87d136254662d04f027
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-helm-cve-2026-35204-8.0/?sphrase_id=1506217
- https://bdu.fstec.ru/vul/2026-07346

3

Краткое описание: Выполнение произвольного кода в РЕД ОС

Идентификатор уязвимости: CVE-2026-32241
BDU:2026-07361

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: РЕД ОС: 8.0
Flannel: до 0.28.2

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://github.com/flannel-io/flannel/releases/tag/v0.28.2
- https://github.com/flannel-io/flannel
- https://github.com/flannel-io/flannel/commit/08bc9a4c990ae785d2fcb448f4991b58485cd26a
- https://github.com/flannel-io/flannel/security/advisories/GHSA-vchx-5pr6-ffx2
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-32241
- https://bdu.fstec.ru/vul/2026-07361

4

Краткое описание: Отказ в обслуживании в РЕД ОС

Идентификатор уязвимости: CVE-2026-27623
BDU:2026-07362

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: РЕД ОС: 8.0
Valkey: до 9.0.3

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://github.com/valkey-io/valkey/security/advisories/GHSA-93p9-5vc7-8wgr
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-27623
- https://bdu.fstec.ru/vul/2026-07362

Краткое описание: Отказ в обслуживании в РЕД ОС

Идентификатор уязвимости: CVE-2026-31899
BDU:2026-07364

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: РЕД ОС: 8.0
CairoSVG: до 2.9.0

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

5

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://github.com/Kozea/CairoSVG
- https://github.com/Kozea/CairoSVG/commit/6dde8685ed3f19837767bce7a13a5491e3d0e0bf
- https://github.com/Kozea/CairoSVG/security/advisories/GHSA-f38f-5xpm-9r7c
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-31899
- https://bdu.fstec.ru/vul/2026-07364

6

Краткое описание: Выполнение произвольного кода в Drupal

Идентификатор уязвимости: CVE-2026-6366
BDU:2026-07320

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: Drupal: от 11.2 до 11.2.11

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-23 / 2026-04-23

Ссылки на источник:

- https://www.drupal.org/sa-core-2026-002
- https://1275.ru/vulnerability/kriticheskaya-uyazvimost-v-drupal-ugrozhaet-millionam-saytov-obnaruzheny-dyry-dlya-udalyonnogo-vypolneniya-koda-i-xss_23701
- https://bdu.fstec.ru/vul/2026-07320

Краткое описание: Повышение привилегий в РЕД ОС

Идентификатор уязвимости: CVE-2026-33898
BDU:2026-07325

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: РЕД ОС: 8.0
Incus: до 6.23.0

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

7

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://github.com/lxc/incus
- https://github.com/lxc/incus/commit/d81d49e746e15dad35de39dc0ace0cedfba7d2f7
- https://github.com/lxc/incus/security/advisories/GHSA-453r-g2pg-cxxq
- https://github.com/lxc/incus/releases/tag/v6.23.0
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-33898
- https://bdu.fstec.ru/vul/2026-07325

8

Краткое описание: Получение конфиденциальной информации в РЕД ОС

Идентификатор уязвимости: CVE-2026-32609
BDU:2026-07330

Идентификатор программной ошибки: CWE-200 Разглашение важной информации лицам без соответствующих прав

Уязвимый продукт: РЕД ОС: 8.0
Glances: до 4.5.2

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Несанкционированный сбор информации.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-25 / 2026-05-25

Ссылки на источник:

- https://github.com/nicolargo/glances/releases/tag/v4.5.2
- https://github.com/nicolargo/glances
- https://github.com/nicolargo/glances/security/advisories/GHSA-cvwp-r2g2-j824
- https://github.com/nicolargo/glances/commit/ff14eb9780ee10ec018c754754b1c8c7bfb6c44f
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-glances-cve-2026-32609-8.0/?sphrase_id=1508829
- https://bdu.fstec.ru/vul/2026-07330

9

Краткое описание: Повышение привилегий в Apex One

Идентификатор уязвимости: CVE-2026-34930
BDU:2026-07433

Идентификатор программной ошибки: CWE-346 Уязвимости, связанные с проверкой источника

Уязвимый продукт: Apex One: до 14.0.20731 (SaaS)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://success.trendmicro.com/en-US/solution/KA-0023430
- https://www.zerodayinitiative.com/advisories/upcoming/
- https://bdu.fstec.ru/vul/2026-07433

10

Краткое описание: Повышение привилегий в Apex One

Идентификатор уязвимости: CVE-2026-45207
BDU:2026-07431

Идентификатор программной ошибки: CWE-346 Уязвимости, связанные с проверкой источника

Уязвимый продукт: Apex One: до 14.0.20731 (SaaS)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://success.trendmicro.com/en-US/solution/KA-0023430
- https://www.zerodayinitiative.com/advisories/upcoming/
- https://bdu.fstec.ru/vul/2026-07431

11

Краткое описание: Повышение привилегий в Apex One

Идентификатор уязвимости: CVE-2026-45208
BDU:2026-07430

Идентификатор программной ошибки: CWE-367 Состояние гонки, связанное со временем проверки и временем использования

Уязвимый продукт: Apex One: до 14.0.20731 (SaaS)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://success.trendmicro.com/en-US/solution/KA-0023430
- https://www.zerodayinitiative.com/advisories/upcoming/
- https://bdu.fstec.ru/vul/2026-07430

Краткое описание: Повышение привилегий в Apex One

Идентификатор уязвимости: CVE-2026-45206
BDU:2026-07436

Идентификатор программной ошибки: CWE-346 Уязвимости, связанные с проверкой источника

Уязвимый продукт: Apex One: до 14.0.20731 (SaaS)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

12

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://success.trendmicro.com/en-US/solution/KA-0023430
- https://bdu.fstec.ru/vul/2026-07436

13

Краткое описание: Повышение привилегий в Apex One

Идентификатор уязвимости: CVE-2026-34929
BDU:2026-07429

Идентификатор программной ошибки: CWE-346 Уязвимости, связанные с проверкой источника

Уязвимый продукт: Apex One: до 14.0.20731 (SaaS)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://success.trendmicro.com/en-US/solution/KA-0023430
- https://www.zerodayinitiative.com/advisories/upcoming/
- https://bdu.fstec.ru/vul/2026-07429

14

Краткое описание: Повышение привилегий в Apex One

Идентификатор уязвимости: CVE-2026-34927
BDU:2026-07437

Идентификатор программной ошибки: CWE-346 Уязвимости, связанные с проверкой источника

Уязвимый продукт: Apex One: до 14.0.20731 (SaaS)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://success.trendmicro.com/en-US/solution/KA-0023430
- https://www.zerodayinitiative.com/advisories/upcoming/
- https://bdu.fstec.ru/vul/2026-07437

15

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-8092
BDU:2026-07463

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Firefox: до 150.0.2
Firefox ESR: до 115.35.2
Thunderbird: до 140.10.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1806249
- https://www.mozilla.org/security/advisories/mfsa2026-40/
- https://www.mozilla.org/security/advisories/mfsa2026-41/
- https://www.mozilla.org/security/advisories/mfsa2026-42/
- https://www.mozilla.org/security/advisories/mfsa2026-43/
- https://www.mozilla.org/security/advisories/mfsa2026-44/
- https://bdu.fstec.ru/vul/2026-07463

Краткое описание: Выполнение произвольного кода в RoundCube Webmail

Идентификатор уязвимости: CVE-2026-48844
BDU:2026-07446

Идентификатор программной ошибки: CWE-670 Некорректная реализация хода выполнения команд

Уязвимый продукт: RoundCube Webmail: от 1.7 до 1.7.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

16

Оценка CVSSv3: 7.5 AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://github.com/roundcube/roundcubemail/commit/6a777d7394b763ce9acfce86c1a521e14a02d862
- https://github.com/roundcube/roundcubemail/commit/ea1798a6fbf060abcc0ba73b2435036bf8016a5a
- https://github.com/roundcube/roundcubemail/releases/tag/1.6.16
- https://github.com/roundcube/roundcubemail/releases/tag/1.7.1
- https://roundcube.net/news/2026/05/24/security-updates-1.6.16-and-1.7.1
- https://bdu.fstec.ru/vul/2026-07446

17

Краткое описание: Выполнение произвольного кода в RoundCube Webmail

Идентификатор уязвимости: CVE-2026-48842
BDU:2026-07447

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: RoundCube Webmail: от 1.7 до 1.7.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://github.com/roundcube/roundcubemail/commit/3406183a9976e36f992d3468f37d0e2346526ee9
- https://github.com/roundcube/roundcubemail/commit/87124cc7136a48b5fa9d2b40dfead6e9dcaeaf4b
- https://github.com/roundcube/roundcubemail/releases/tag/1.6.16
- https://github.com/roundcube/roundcubemail/releases/tag/1.7.1
- https://roundcube.net/news/2026/05/24/security-updates-1.6.16-and-1.7.1
- https://bdu.fstec.ru/vul/2026-07447

Краткое описание: Получение конфиденциальной информации в Firefox

Идентификатор уязвимости: CVE-2026-7320
BDU:2026-07459

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Firefox: до 150.0.1
Firefox ESR: до 140.10.1
Thunderbird: до 140.10.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

18

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://bugzilla.mozilla.org/show_bug.cgi?id=2027433
- https://www.mozilla.org/security/advisories/mfsa2026-35/
- https://www.mozilla.org/security/advisories/mfsa2026-36/
- https://www.mozilla.org/security/advisories/mfsa2026-37/
- https://www.mozilla.org/security/advisories/mfsa2026-38/
- https://www.mozilla.org/security/advisories/mfsa2026-39/
- https://bdu.fstec.ru/vul/2026-07459

Краткое описание: Выполнение произвольного кода в N300RH

Идентификатор уязвимости: CVE-2026-9543
BDU:2026-07424

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: N300RH: 6.1c.1353_B20190305

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

19

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-28 / 2026-05-28

Ссылки на источник:

- https://github.com/A1ester/TOTOLINK-N300RH-Command-Injection
- https://github.com/A1ester/TOTOLINK-N300RH-Command-Injection/blob/main/TOTOLINK%20N300RH%20Command%20Injection%20Vulnerability.md
- https://vuldb.com/submit/815068
- https://bdu.fstec.ru/vul/2026-07424

20

Краткое описание: Повышение привилегий в Apex One

Идентификатор уязвимости: CVE-2026-34928
BDU:2026-07438

Идентификатор программной ошибки: CWE-346 Уязвимости, связанные с проверкой источника

Уязвимый продукт: Apex One: до 14.0.20731 (SaaS)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://success.trendmicro.com/en-US/solution/KA-0023430
- https://www.zerodayinitiative.com/advisories/upcoming/
- https://bdu.fstec.ru/vul/2026-07438

Краткое описание: Выполнение произвольного кода в Tenda F1202

Идентификатор уязвимости: CVE-2026-9431
BDU:2026-07398

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda F1202: 1.2.0.20(408)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

21 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-27 / 2026-05-27

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new2/blob/main/F1202/vul_35/README.md
- https://bdu.fstec.ru/vul/2026-07398

Краткое описание: Выполнение произвольного кода в PAN-OS

Идентификатор уязвимости: CVE-2026-0263
BDU:2026-07382

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PAN-OS: до 11.1.15

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

22 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-25 / 2026-05-25

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0263
- https://bdu.fstec.ru/vul/2026-07382

Краткое описание: Выполнение произвольного кода в Tenda F1202

Идентификатор уязвимости: CVE-2026-9429
BDU:2026-07394

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda F1202: 1.2.0.20(408)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

23

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-27 / 2026-05-27

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new2/blob/main/F1202/vul_31/README.md
- https://bdu.fstec.ru/vul/2026-07394

Краткое описание: Выполнение произвольного кода в Tenda F1202

Идентификатор уязвимости: CVE-2026-9428
BDU:2026-07392

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda F1202: 1.2.0.20(408)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

24

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-27 / 2026-05-27

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new2/blob/main/F1202/vul_29/README.md
- https://bdu.fstec.ru/vul/2026-07392

Краткое описание: Выполнение произвольного кода в Tenda F1202

Идентификатор уязвимости: CVE-2026-9430
BDU:2026-07396

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda F1202: 1.2.0.20(408)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

25

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-27 / 2026-05-27

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new2/blob/main/F1202/vul_32/README.md
- https://bdu.fstec.ru/vul/2026-07396

Краткое описание: Получение конфиденциальной информации в CXF

Идентификатор уязвимости: CVE-2026-44930
BDU:2026-07399

Идентификатор программной ошибки: CWE-90 Некорректная нейтрализация специальных элементов, используемых в LDAP-запросах (внедрение LDAP)

Уязвимый продукт: CXF: до 3.6.11

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Получение конфиденциальной информации

26 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-27 / 2026-05-27

Ссылки на источник:

- https://lists.apache.org/thread/c1zqxppo1m5z3kbdhjn5p991zk09ynkh
- https://www.openwall.com/lists/oss-security/2026/05/22/9
- https://bdu.fstec.ru/vul/2026-07399

27

Краткое описание: Получение конфиденциальной информации в Gitea

Идентификатор уязвимости: CVE-2026-27771
BDU:2026-07479

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: Gitea: до 1.26.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-28 / 2026-05-28

Ссылки на источник:

- https://github.com/portbuster1337/CVE-2026-27771
- https://www.noscope.com/blog/gitea-instances-exposing-private-container
- https://github.com/go-gitea/gitea/security/advisories
- https://github.com/go-gitea/gitea/pull/37610
- https://github.com/go-gitea/gitea/pull/37290
- https://blog.gitea.com/release-of-1.26.2/
- https://orca.security/resources/blog/gitea-container-registry-vulnerability/
- https://bdu.fstec.ru/vul/2026-07479

28

Краткое описание: Внедрение кода в Gitlab

Идентификатор уязвимости: CVE-2026-4868
BDU:2026-07488

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: Gitlab: от 18.8.0 до 18.10.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Внедрение кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-28 / 2026-05-28

Ссылки на источник:

- https://about.gitlab.com/releases/2026/05/27/patch-release-gitlab-19-0-1-released/
- https://hackerone.com/reports/3619872
- https://bdu.fstec.ru/vul/2026-07488

29

Краткое описание: Выполнение произвольного кода в Tenda F456

Идентификатор уязвимости: CVE-2026-7081
BDU:2026-07515

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: Tenda F456: 1.0.0.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_133/README.md
- https://bdu.fstec.ru/vul/2026-07515

Краткое описание: Выполнение произвольного кода в Tenda F456

Идентификатор уязвимости: CVE-2026-7082
BDU:2026-07514

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: Tenda F456: 1.0.0.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

30

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_134/README.md
- https://vuldb.com/submit/798465
- https://bdu.fstec.ru/vul/2026-07514

Краткое описание: Выполнение произвольного кода в Tenda F451

Идентификатор уязвимости: CVE-2026-5992
BDU:2026-07513

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: F451: 1.0.0.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

31

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/Jimi-Lab/cve/issues/9
- https://vuldb.com/submit/792862
- https://vuldb.com/vuln/356545
- https://vuldb.com/vuln/356545/cti
- https://www.tenda.com.cn/
- https://bdu.fstec.ru/vul/2026-07513

Краткое описание: Выполнение произвольного кода в Tenda HG9

Идентификатор уязвимости: CVE-2026-2905
BDU:2026-07512

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda HG9: 300001138

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

32 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/QIU-DIE/cve-nneeww/issues/7
- https://bdu.fstec.ru/vul/2026-07512

Краткое описание: Отказ в обслуживании в Tenda F451

Идентификатор уязвимости: CVE-2026-5990
BDU:2026-07510

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: F451: 1.0.0.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

33

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/Jimi-Lab/cve/issues/8
- https://vuldb.com/submit/792861
- https://vuldb.com/vuln/356544
- https://vuldb.com/vuln/356544/cti
- https://www.tenda.com.cn/
- https://bdu.fstec.ru/vul/2026-07510

34

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-5997
BDU:2026-07509

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_169/README.md
- https://vuldb.com/submit/792045
- https://vuldb.com/vuln/356551
- https://vuldb.com/vuln/356551/cti
- https://www.totolink.net/
- https://bdu.fstec.ru/vul/2026-07509

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-5996
BDU:2026-07508

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

35

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_168/README.md
- https://vuldb.com/submit/792044
- https://vuldb.com/vuln/356550
- https://vuldb.com/vuln/356550/cti
- https://www.totolink.net/
- https://bdu.fstec.ru/vul/2026-07508

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-5995
BDU:2026-07507

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

36

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_167/README.md
- https://vuldb.com/submit/792043
- https://vuldb.com/vuln/356549
- https://vuldb.com/vuln/356549/cti
- https://www.totolink.net/
- https://bdu.fstec.ru/vul/2026-07507

37

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-5993
BDU:2026-07506

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_165/README.md
- https://vuldb.com/submit/792041
- https://vuldb.com/vuln/356547
- https://vuldb.com/vuln/356547/cti
- https://www.totolink.net/
- https://bdu.fstec.ru/vul/2026-07506

Краткое описание: Отказ в обслуживании в Tenda F451

Идентификатор уязвимости: CVE-2026-5991
BDU:2026-07511

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: F451: 1.0.0.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

38

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/Jimi-Lab/cve/issues/9
- https://vuldb.com/submit/792862
- https://vuldb.com/vuln/356545
- https://vuldb.com/vuln/356545/cti
- https://www.tenda.com.cn/
- https://bdu.fstec.ru/vul/2026-07511

Краткое описание: Выполнение произвольного кода в DWR-M960

Идентификатор уязвимости: CVE-2026-2927
BDU:2026-07504

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DWR-M960: 1.01.07

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

39

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/LX-66-LX/cve-new/issues/22
- https://bdu.fstec.ru/vul/2026-07504

40

Краткое описание: Выполнение произвольного кода в Gogs

Идентификатор уязвимости: BDU:2026-07491

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: Gogs: 0.15.0+dev

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-29 / 2026-05-29

Ссылки на источник:

- https://www.rapid7.com/blog/post/ve-authenticated-rce-via-argument-injection-gogs-unfixed/
- https://bdu.fstec.ru/vul/2026-07491

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-5994
BDU:2026-07505

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

41

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_166/README.md
- https://vuldb.com/submit/792042
- https://vuldb.com/vuln/356548
- https://vuldb.com/vuln/356548/cti
- https://www.totolink.net/
- https://bdu.fstec.ru/vul/2026-07505

Краткое описание: Выполнение произвольного кода в Notepad++

Идентификатор уязвимости: CVE-2026-48778
BDU:2026-07493

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: Notepad++: до 8.9.6.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения
42 только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-29 / 2026-05-29

Ссылки на источник:

- https://www.acn.gov.it/portale/w/notepad-poc-pubblici-per-le-cve-2026-48800-cve-2026-48778-e-cve-2026-48770
- https://notepad-plus-plus.org/news/v8961-released/
- https://community.notepad-plus-plus.org/topic/27548/notepad-release-8.9.6.1
- https://github.com/notepad-plus-plus/notepad-plus-plus/security/advisories/GHSA-7hm3-wp5q-ccv9
- https://bdu.fstec.ru/vul/2026-07493

Краткое описание: Выполнение произвольного кода в Notepad++

Идентификатор уязвимости: CVE-2026-48800
BDU:2026-07494

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: Notepad++: до 8.9.6.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

43

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-29 / 2026-05-29

Ссылки на источник:

- https://www.acn.gov.it/portale/w/notepad-poc-pubblici-per-le-cve-2026-48800-cve-2026-48778-e-cve-2026-48770
- https://notepad-plus-plus.org/news/v8961-released/
- https://community.notepad-plus-plus.org/topic/27548/notepad-release-8.9.6.1
- https://github.com/notepad-plus-plus/notepad-plus-plus/security/advisories/GHSA-3x3f-3j39-pj3v
- https://bdu.fstec.ru/vul/2026-07494

Краткое описание: Отказ в обслуживании в crypto

Идентификатор уязвимости: CVE-2026-39829
BDU:2026-07495

Идентификатор программной ошибки: CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

Уязвимый продукт: crypto: до 0.52.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

44

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-27 / 2026-05-27

Ссылки на источник:

- https://pkg.go.dev/vuln/GO-2026-5018
- https://go-review.googlesource.com/c/crypto/+/781641
- https://go-review.googlesource.com/c/crypto/+/781661
- https://github.com/golang/go/issues/79565
- https://groups.google.com/g/golang-announce/c/a082jnz-Lvl
- https://bdu.fstec.ru/vul/2026-07495

Краткое описание: Выполнение произвольного кода в Tenda HG9

Идентификатор уязвимости: CVE-2026-2910
BDU:2026-07497

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda HG9: 300001138

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

45

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-25 / 2026-05-25

Ссылки на источник:

- https://github.com/QIU-DIE/cve-nneeww/issues/12
- https://bdu.fstec.ru/vul/2026-07497

Краткое описание: Выполнение произвольного кода в Tenda HG9

Идентификатор уязвимости: CVE-2026-2909
BDU:2026-07496

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda HG9: 300001138

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

46

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-25 / 2026-05-25

Ссылки на источник:

- https://github.com/QIU-DIE/cve-nneeww/issues/11
- https://bdu.fstec.ru/vul/2026-07496

Краткое описание: Выполнение произвольного кода в DIR-825M

Идентификатор уязвимости: CVE-2026-7288
BDU:2026-07500

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: DIR-825M: 1.1.12

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

47

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-19 / 2026-05-19

Ссылки на источник:

- https://github.com/Kiciot/cve/issues/2
- https://vuldb.com/submit/803024
- https://vuldb.com/vuln/359946
- https://vuldb.com/vuln/359946/cti
- https://www.dlink.com/
- https://bdu.fstec.ru/vul/2026-07500

Краткое описание: Выполнение произвольного кода в DIR-825M

Идентификатор уязвимости: CVE-2026-7289
BDU:2026-07501

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: DIR-825M: 1.1.12

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

48

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-19 / 2026-05-19

Ссылки на источник:

- https://github.com/Kiciot/cve/issues/3
- https://vuldb.com/submit/803025
- https://vuldb.com/vuln/359947
- https://vuldb.com/vuln/359947/cti
- https://www.dlink.com/
- https://bdu.fstec.ru/vul/2026-07501

Краткое описание: Выполнение произвольного кода в DWR-M960

Идентификатор уязвимости: CVE-2026-2929
BDU:2026-07502

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DWR-M960: 1.01.07

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

49

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/LX-66-LX/cve-new/issues/24
- https://bdu.fstec.ru/vul/2026-07502

Краткое описание: Отказ в обслуживании в DWR-M960

Идентификатор уязвимости: CVE-2026-2926
BDU:2026-07503

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DWR-M960: 1.01.07

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

50

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-05 / 2026-05-05

Ссылки на источник:

- https://github.com/LX-66-LX/cve-new/issues/21
- https://bdu.fstec.ru/vul/2026-07503

Краткое описание: Выполнение произвольного кода в Tenda HG9

Идентификатор уязвимости: CVE-2026-2908
BDU:2026-07498

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda HG9: 300001138

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

51

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-25 / 2026-05-25

Ссылки на источник:

- https://github.com/QIU-DIE/cve-nneeww/issues/10
- https://bdu.fstec.ru/vul/2026-07498

52

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-6026
BDU:2026-07596

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-14 / 2026-04-14

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_171/README.md
- https://bdu.fstec.ru/vul/2026-07596

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-6027
BDU:2026-07599

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

53

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-14 / 2026-04-14

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_172/README.md
- https://bdu.fstec.ru/vul/2026-07599

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-6025
BDU:2026-07598

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

54

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-14 / 2026-04-14

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_170/README.md
- https://bdu.fstec.ru/vul/2026-07598

55

Краткое описание: Отказ в обслуживании в A800R

Идентификатор уязвимости: CVE-2026-6157
BDU:2026-07597

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: A800R: 4.1.2cu.5137_B20200730

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-14 / 2026-04-14

Ссылки на источник:

- https://github.com/xyh4ck/iot_poc/blob/main/TOTOLINK/A800R/01_Buffer_Overflow_setAppEasyWizardConfig.md
- https://bdu.fstec.ru/vul/2026-07597

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-6156
BDU:2026-07595

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

56

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-14 / 2026-04-14

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_197/README.md
- https://bdu.fstec.ru/vul/2026-07595

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-6028
BDU:2026-07593

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

57

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-14 / 2026-04-14

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_173/README.md
- https://bdu.fstec.ru/vul/2026-07593

58

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-6132
BDU:2026-07592

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-14 / 2026-04-14

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_183/README.md
- https://bdu.fstec.ru/vul/2026-07592

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-6155
BDU:2026-07591

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

59

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-14 / 2026-04-14

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_196/README.md
- https://bdu.fstec.ru/vul/2026-07591

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-6029
BDU:2026-07600

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

60

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-14 / 2026-04-14

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_174/README.md
- https://vuldb.com/submit/792050
- https://bdu.fstec.ru/vul/2026-07600

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-6154
BDU:2026-07594

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

61

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-14 / 2026-04-14

Ссылки на источник:

- https://dbugs.ptsecurity.com/vulnerability/PT-2026-32239
- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_194/README.md
- https://bdu.fstec.ru/vul/2026-07594

62

Краткое описание: Выполнение произвольного кода в A7100RU

Идентификатор уязвимости: CVE-2026-6195
BDU:2026-07602

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: A7100RU: 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-07 / 2026-04-07

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_198/README.md
- https://bdu.fstec.ru/vul/2026-07602

Краткое описание: Выполнение произвольного кода в Megatron-LM

Идентификатор уязвимости: CVE-2026-24150
BDU:2026-07616

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Megatron-LM: до 0.15.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

63

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-31 / 2026-03-31

Ссылки на источник:

- https://www.cve.org/CVERecord?idCVE-2026-24150
- https://nvd.nist.gov/vuln/detail/CVE-2026-24150
- https://nvidia.custhelp.com/app/answers/detail/a_id/5769
- https://bdu.fstec.ru/vul/2026-07616

Краткое описание: Выполнение произвольного кода в MongoDB

Идентификатор уязвимости: CVE-2026-8053
BDU:2026-07604

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: MongoDB: от 5.0.0 до 5.0.32 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

64

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://jira.mongodb.org/browse/SERVER-126021
- https://sploitus.com/exploit?id=6F3CBDD6-D539-546A-BE8F-2A0BD44EF01D
- https://github.com/advisories/ghsa-pr63-cc36-q84h
- https://github.com/mgiay/CVE-2026-8053-MongoDB
- https://bdu.fstec.ru/vul/2026-07604

Краткое описание: Отказ в обслуживании в LR350

Идентификатор уязвимости: CVE-2026-4976
BDU:2026-07611

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: LR350: 9.3.5u.6369_B20220309

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

65

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-02 / 2026-04-02

Ссылки на источник:

- https://lavender-bicycle-a5a.notion.site/TOTOLINK-LR350-setWiFiGuestCfg-32153a41781f8048a918c1c78e95064e
- https://lavender-bicycle-a5a.notion.site/TOTOLINK-LR350-setWiFiGuestCfg-32153a41781f8048a918c1c78e95064e?source=copy_link
- https://bdu.fstec.ru/vul/2026-07611

66

Краткое описание: Выполнение произвольного кода в Megatron-LM

Идентификатор уязвимости: CVE-2026-24152
BDU:2026-07615

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Megatron-LM: до 0.15.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-31 / 2026-03-31

Ссылки на источник:

- https://www.cve.org/CVERecord?idCVE-2026-24152
- https://nvidia.custhelp.com/app/answers/detail/a_id/5769
- https://bdu.fstec.ru/vul/2026-07615

Краткое описание: Получение конфиденциальной информации в moodle-mod_customcert

Идентификатор уязвимости: CVE-2026-30884
BDU:2026-07583

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: moodle-mod_customcert: до 5.0.2 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

67

Оценка CVSSv3: 9.6 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-18 / 2026-03-18

Ссылки на источник:

- https://github.com/mdjnelson/moodle-mod_customcert/security/advisories/GHSA-8pjr-j7r4-ccjx
- https://github.com/mdjnelson/moodle-mod_customcert/commit/a1494a80fb953f187f7888a7394cbf9d13c28468
- https://github.com/mdjnelson/moodle-mod_customcert/commit/ddc8f01f1e19fb61202f6013a38ef757486d3ba0
- https://bdu.fstec.ru/vul/2026-07583

68

Краткое описание: Выполнение произвольного кода в Megatron-LM

Идентификатор уязвимости: CVE-2026-24151
BDU:2026-07617

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Megatron-LM: до 0.15.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-31 / 2026-03-31

Ссылки на источник:

- https://www.cve.org/CVERecord?idCVE-2026-24151
- https://nvidia.custhelp.com/app/answers/detail/a_id/5769
- https://bdu.fstec.ru/vul/2026-07617

Краткое описание: Выполнение произвольного кода в TRENDnet TEW-432BRP

Идентификатор уязвимости: CVE-2026-10161
BDU:2026-07556

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TRENDnet TEW-432BRP: 3.10B20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

69

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://github.com/wudipjq/my_vuln/blob/main/TRENDnet/vuln_14/14.md
- https://bdu.fstec.ru/vul/2026-07556

70

Краткое описание: Выполнение произвольного кода в CX17NF-WF

Идентификатор уязвимости: CVE-2020-36984
BDU:2026-07526

Идентификатор программной ошибки: CWE-428 Отсутствие кавычек вокруг элемента в пути поиска

Уязвимый продукт: CX17NF-WF: 1.124

Категория уязвимого продукта: Периферийное оборудование

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-02 / 2026-02-02

Ссылки на источник:

- https://www.epson.co.uk/en_GB/support/sc/epson-aculaser-cx17nf-wf/s/s1068#drivers_and_manuals
- https://www.exploit-db.com/exploits/48965
- https://bdu.fstec.ru/vul/2026-07526

71

Краткое описание: Выполнение произвольного кода в Thymeleaf

Идентификатор уязвимости: CVE-2026-41901
BDU:2026-07527

Идентификатор программной ошибки: CWE-1039 Некорректная работа автоматизированного механизма распознавания при определении или обработке входных данных, модифицированных злоумышленником

Уязвимый продукт: Thymeleaf: до 3.1.5.RELEASE

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-27 / 2026-05-27

Ссылки на источник:

- https://github.com/thymeleaf/thymeleaf/security/advisories/GHSA-c9ph-gxww-7744
- https://github.com/thymeleaf/thymeleaf/releases/tag/thymeleaf-3.1.5.RELEASE
- https://github.com/HORKimhab/CVE-2026-41901
- https://bdu.fstec.ru/vul/2026-07527

Краткое описание: Межсайтовый скриптинг в pimcore

Идентификатор уязвимости: CVE-2024-11954
BDU:2026-07528

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: pimcore: от 11.4.2 до 11.5.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Межсайтовый скриптинг

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

72

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-02-06 / 2025-02-06

Ссылки на источник:

- https://osv.dev/vulnerability/GHSA-xr3m-6gq6-22cg
- https://github.com/advisories/GHSA-xr3m-6gq6-22cg
- https://github.com/github/advisory-database/blob/main/advisories/github-reviewed/2025/01/GHSA-xr3m-6gq6-22cg/GHSA-xr3m-6gq6-22cg.json
- https://bdu.fstec.ru/vul/2026-07528

73

Краткое описание: Отказ в обслуживании в Mattermost

Идентификатор уязвимости: CVE-2026-5740
BDU:2026-07533

Идентификатор программной ошибки: CWE-789 Неконтролируемое выделение памяти

Уязвимый продукт: Mattermost: от 11.6.0 до 11.6.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-27 / 2026-05-27

Ссылки на источник:

- https://mattermost.com/security-updates
- https://vuldb.com/vuln/365177
- https://bdu.fstec.ru/vul/2026-07533

Краткое описание: Отказ в обслуживании в Mattermost

Идентификатор уязвимости: CVE-2026-5308
BDU:2026-07536

Идентификатор программной ошибки: CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

Уязвимый продукт: Mattermost: от 11.6.0 до 11.6.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Отказ в обслуживании

74 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-27 / 2026-05-27

Ссылки на источник:

- https://mattermost.com/security-updates
- https://bdu.fstec.ru/vul/2026-07536

Краткое описание: Повышение привилегий в Ubuntu

Идентификатор уязвимости: CVE-2026-34177
BDU:2026-07537

Идентификатор программной ошибки: CWE-184 Неполный черный список

Уязвимый продукт: Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
РЕД ОС: 8.0
LXD: от 4.12 до 6.8

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

75

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-29 / 2026-05-29

Ссылки на источник:

- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-34177
- https://github.com/canonical/lxd/pull/17909
- https://github.com/canonical/lxd
- https://github.com/canonical/lxd/security/advisories/GHSA-fm2x-c5qw-4h6f
- https://security-tracker.debian.org/tracker/CVE-2026-34177
- https://ubuntu.com/security/CVE-2026-34177
- https://bdu.fstec.ru/vul/2026-07537

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2026-34178
BDU:2026-07538

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
РЕД ОС: 8.0
LXD: от 4.12 до 6.8

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

76

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-29 / 2026-05-29

Ссылки на источник:

- https://github.com/canonical/lxd/security/advisories/GHSA-q96j-3fmm-7fv4
- https://github.com/canonical/lxd
- https://github.com/canonical/lxd/pull/17921
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-34178
- https://security-tracker.debian.org/tracker/CVE-2026-34178
- https://ubuntu.com/security/CVE-2026-34178
- https://bdu.fstec.ru/vul/2026-07538

77

Краткое описание: Повышение привилегий в Ubuntu

Идентификатор уязвимости: CVE-2026-34179
BDU:2026-07539

Идентификатор программной ошибки: CWE-915 Некорректный контроль над изменением динамически определяемых атрибутов объектов

Уязвимый продукт: Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
РЕД ОС: 8.0
Incus: до 6.23.0
LXD: от 4.12 до 6.8

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-29 / 2026-05-29

Ссылки на источник:

- https://github.com/canonical/lxd/security/advisories/GHSA-c3h3-89qf-jqm5
- https://github.com/canonical/lxd/pull/17936
- https://security-tracker.debian.org/tracker/CVE-2026-34179
- https://ubuntu.com/security/CVE-2026-34179
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-34179
- https://bdu.fstec.ru/vul/2026-07539

78

Краткое описание: Повышение привилегий в PowerStrip

Идентификатор уязвимости: CVE-2026-29923
BDU:2026-07540

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: PowerStrip: до 3.90.736 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-21 / 2026-04-21

Ссылки на источник:

- https://github.com/Smarttfoxx/CVE-2026-29923
- https://securityvulnerability.io/vulnerability/CVE-2026-29923
- https://bdu.fstec.ru/vul/2026-07540

79

Краткое описание: Выполнение произвольного кода в Metinfo

Идентификатор уязвимости: CVE-2026-29014
BDU:2026-07542

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: Metinfo: от 7.9 до 8.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://karmainsecurity.com/KIS-2026-06
- https://websec.net/blog/cve-2026-29014-metinfo-cms-unauthenticated-php-code-injection-69cdc290c14a8a99e1f91b7a
- https://thehackernews.com/2026/05/metinfo-cms-cve-2026-29014-exploited.html
- https://www.metinfo.cn/news/2875.html
- https://bdu.fstec.ru/vul/2026-07542

80

Краткое описание: Выполнение произвольного кода в Debian GNU/Linux

Идентификатор уязвимости: CVE-2026-33540
BDU:2026-07550

Идентификатор программной ошибки: CWE-918 Подделка запроса со стороны сервера

Уязвимый продукт: Debian GNU/Linux: 13
РЕД ОС: 8.0
Distribution: от 3.0.0 до 3.1.0

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-28 / 2026-05-28

Ссылки на источник:

- https://github.com/advisories/GHSA-3p65-76g6-3w7r
- https://github.com/distribution/distribution/commit/cc5d5fa4ba02157501e6afa2cc6a903ad0338e7b
- https://github.com/distribution/distribution/security/advisories/GHSA-3p65-76g6-3w7r
- https://github.com/distribution/distribution
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-33540
- https://security-tracker.debian.org/tracker/CVE-2026-33540
- https://bdu.fstec.ru/vul/2026-07550

81

Краткое описание: Повышение привилегий в Debian GNU/Linux

Идентификатор уязвимости: CVE-2026-35172
BDU:2026-07552

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Debian GNU/Linux: 13
РЕД ОС: 8.0
Distribution: до 2.8.3 включительно

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-28 / 2026-05-28

Ссылки на источник:

- https://github.com/advisories/GHSA-f2g3-hh2r-cwgc
- https://github.com/distribution/distribution/commit/078b0783f239b4115d1a979e66f08832084e9d1d
- https://github.com/distribution/distribution
- https://github.com/distribution/distribution/security/advisories/GHSA-f2g3-hh2r-cwgc
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-35172
- https://security-tracker.debian.org/tracker/CVE-2026-35172
- https://bdu.fstec.ru/vul/2026-07552

Краткое описание: Выполнение произвольного кода в TRENDnet TEW-432BRP

Идентификатор уязвимости: CVE-2026-10162
BDU:2026-07554

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TRENDnet TEW-432BRP: 3.10B20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

82

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://github.com/wudipjq/my_vuln/blob/main/TRENDnet/vuln_15/15.md
- https://bdu.fstec.ru/vul/2026-07554

Краткое описание: Выполнение произвольного кода в TRENDnet TEW-432BRP

Идентификатор уязвимости: CVE-2026-10160
BDU:2026-07557

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TRENDnet TEW-432BRP: 3.10B20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

83

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- http://github.com/wudipjq/my_vuln/blob/main/TRENDnet/vuln_13/13.md
- https://bdu.fstec.ru/vul/2026-07557

Краткое описание: Выполнение произвольного кода в TRENDnet TEW-432BRP

Идентификатор уязвимости: CVE-2026-10158
BDU:2026-07558

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TRENDnet TEW-432BRP: 3.10B20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

84

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://github.com/wudipjq/my_vuln/blob/main/TRENDnet/vuln_11/11.md
- https://bdu.fstec.ru/vul/2026-07558

Краткое описание: Выполнение произвольного кода в TRENDnet TEW-432BRP

Идентификатор уязвимости: CVE-2026-10159
BDU:2026-07561

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TRENDnet TEW-432BRP: 3.10B20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

85

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://github.com/wudipjq/my_vuln/blob/main/TRENDnet/vuln_12/12.md
- https://bdu.fstec.ru/vul/2026-07561

86

Краткое описание: Отказ в обслуживании в botan

Идентификатор уязвимости: CVE-2026-32877
BDU:2026-07567

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: botan: от 2.3.0 до 3.10.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-08 / 2026-04-08

Ссылки на источник:

- https://github.com/randombit/botan/security/advisories/GHSA-7jj6-4r42-w9h6
- https://www.cybersecurity-help.cz/vdb/vulns/125381/
- https://bdu.fstec.ru/vul/2026-07567

87

Краткое описание: Выполнение произвольного кода в TRENDnet TEW-432BRP

Идентификатор уязвимости: CVE-2026-10120
BDU:2026-07571

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TRENDnet TEW-432BRP: 3.10B20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://github.com/wudipjq/my_vuln/blob/main/TRENDnet/vuln_7/7.md
- https://bdu.fstec.ru/vul/2026-07571

88

Краткое описание: Выполнение произвольного кода в TRENDnet TEW-432BRP

Идентификатор уязвимости: CVE-2026-10119
BDU:2026-07572

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TRENDnet TEW-432BRP: 3.10B20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://github.com/wudipjq/my_vuln/blob/main/TRENDnet/vuln_6/6.md
- https://feedly.com/cve/CVE-2026-10119
- https://bdu.fstec.ru/vul/2026-07572

Краткое описание: Выполнение произвольного кода в Archer C64

Идентификатор уязвимости: CVE-2026-8697
BDU:2026-07573

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: Archer C64: до 1.15.0 Build 250729

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

89

Оценка CVSSv3: 8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-29 / 2026-05-29

Ссылки на источник:

- https://github.com/itzmetanjim/cve-2026-8697
- https://www.tp-link.com/us/support/faq/5105/
- https://vuldb.com/de/cve/CVE-2026-8697
- https://bdu.fstec.ru/vul/2026-07573

90

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46243
BDU:2026-07574

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: Linux: до 7.1 rc5
CentOS: Stream 9
Ubuntu: 22.04
OpenSUSE Leap: 15.6
Linux Mint: 22.3
Suse Linux Enterprise Server: SAP 15 SP7
Debian GNU/Linux: 13
Oracle Linux: 9
Amazon Linux: 2023
AlmaLinux: 9.7
Rocky Linux: 9
Kali Linux: 2026.1

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://heyitsas.im/posts/cifswitch/
- https://github.com/torvalds/linux/commit/3da1fdf4efbc490041eb4f836bf596201203f8f2
- https://github.com/manizada/CIFSwitch/
- https://git.kernel.org/stable/c/0aece6685fc80a8de492688ca2315fb86ec379c7
- https://git.kernel.org/stable/c/2035acfb17221729b1b8ac335e941868a04ca079
- https://git.kernel.org/stable/c/3da1fdf4efbc490041eb4f836bf596201203f8f2
- https://git.kernel.org/stable/c/7713bd320ed4fc3d08a227cd8e41242219a16981
- https://git.kernel.org/stable/c/91f89c1d83e80417629791fcef6af8140d7d01c8
- https://git.kernel.org/stable/c/9544559e59438a4b609b2fdfa0763d8360572824
- https://git.kernel.org/stable/c/a3bbda6502a9398b816fa2e71c9a3f955f58013d
- https://git.kernel.org/stable/c/cf20038657d6d4974349556a34e08fe0490bebbc
- https://security-tracker.debian.org/tracker/CVE-2026-46243
- https://bdu.fstec.ru/vul/2026-07574

91

Краткое описание: Выполнение произвольного кода в LibreOffice AgileEngine

Идентификатор уязвимости: CVE-2026-4430
BDU:2026-06581

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: LibreOffice: 25.2.0.1 - 26.2.2.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Запись за пределами буфера.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: 5.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://www.libreoffice.org/about-us/security/advisories/CVE-2026-4430/

92

Краткое описание: Выполнение произвольного кода в Magic Collaboration Studio

Идентификатор уязвимости: CVE-2026-7858

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Magic Collaboration Studio: все версии
No Magic: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://www.3ds.com/trust-center/security/security-advisories/cve-2026-7858

93

Краткое описание: Выполнение произвольного кода в TanStack

Идентификатор уязвимости: CVE-2026-45321
BDU:2026-06725

Идентификатор программной ошибки: CWE-506 Внедренный вредоносный код

Уязвимый продукт: eslint-plugin-start: 0.0.4, 0.0.7
react-start-rsc: 0.0.47, 0.0.50
nitro-v2-vite-plugin: 1.154.12, 1.154.15
start-fn-stubs: 1.161.9, 1.161.12
eslint-plugin-router: 1.161.9, 1.161.12
history: 1.161.9, 1.161.12
virtual-file-routes: 1.161.10, 1.161.13
router-utils: 1.161.11, 1.161.14
arktype-adapter: 1.166.12, 1.166.15
valibot-adapter: 1.166.12, 1.166.15
zod-adapter: 1.166.12, 1.166.15
solid-router-ssr-query: 1.166.15, 1.166.18
vue-router-ssr-query: 1.166.15, 1.166.18
react-router-ssr-query: 1.166.15, 1.166.18
vue-router-devtools: 1.166.16, 1.166.19
solid-router-devtools: 1.166.16, 1.166.19
react-router-devtools: 1.166.16, 1.166.19
router-devtools: 1.166.16, 1.166.19
start-storage-context: 1.166.38, 1.166.41
start-static-server-functions: 1.166.44, 1.166.47
router-generator: 1.166.45, 1.166.48
router-cli: 1.166.46, 1.166.49
vue-start-client: 1.166.46, 1.166.49
vue-start-server: 1.166.50, 1.166.53
solid-start-client: 1.166.50, 1.166.53
react-start-client: 1.166.51, 1.166.54
router-vite-plugin: 1.166.53, 1.166.56
solid-start-server: 1.166.54, 1.166.57
react-start-server: 1.166.55, 1.166.58

router-devtools-core: 1.167.6, 1.167.9
start-server-core: 1.167.33, 1.167.36
router-plugin: 1.167.38, 1.167.41
vue-start: 1.167.61, 1.167.64
solid-start: 1.167.65, 1.167.68
react-start: 1.167.68, 1.167.71
router-ssr-query-core: 1.168.3, 1.168.6
start-client-core: 1.168.5, 1.168.8
vue-router: 1.169.5, 1.169.8
solid-router: 1.169.5, 1.169.8
router-core: 1.169.5, 1.169.8
react-router: 1.169.5, 1.169.8
start-plugin-core: 1.169.23, 1.169.26

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-29 / 2026-05-29

Ссылки на источник:

- https://github.com/advisories/GHSA-g7cv-rxg3-hmpx
- https://github.com/TanStack/router/issues/7383

94

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2026-10701

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Mozilla Firefox: 150.0 - 151.0.2
Firefox for Android: 150.0 - 151.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Запись за пределами буфера.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-03 / 2026-06-03

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-54/
- https://bugzilla.mozilla.org/show_bug.cgi?id=2038537
- https://bugzilla.mozilla.org/show_bug.cgi?id=2040903