НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-06-16.1 | 16 июня 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-42835	Microsoft Teams for Android	Сетевой	DoS	2026-06-09	✓
2	Критическая	CVE-2026-25089	FortiSandbox	Сетевой	ACE	2026-06-09	✓
3	Критическая	CVE-2026-40128	SAP NetWeaver Application Server Java Web Container	Сетевой	ACE	2026-06-09	✓
4	Высокая	CVE-2026-34126	TP-Link products	Смежная сеть	OSI	2026-06-08	✓
5	Высокая	CVE-2026-44825	Apache Solr	Сетевой	PE	2026-06-04	✓
6	Высокая	CVE-2026-49975	Microsoft IIS HTTP/2 support	Сетевой	DoS	2026-06-04	✗
7	Критическая	CVE-2026-46244	Linux kernel netfilter	Сетевой	SB	2026-06-04	✓
8	Критическая	CVE-2026-45247	Mirasvit Cache Warmer for Magento 2	Сетевой	ACE	2026-06-04	✓
9	Критическая	CVE-2026-46266	Linux kernel ipv6	Сетевой	SB	2026-06-04	✓
10	Высокая	CVE-2026-25936	GLPI Project	Сетевой	ACE	2026-05-28	✓
11	Критическая	CVE-2026-40342	Firebird	Сетевой	ACE	2026-04-22	✓
12	Высокая	CVE-2026-25673	Django	Сетевой	DoS	2026-05-28	✓
13	Высокая	CVE-2026-33034	Ubuntu	Сетевой	DoS	2026-05-28	✓

14	Критическая	CVE-2026-4277	Ubuntu	Сетевой	OSI	2026-06-03	✓
15	Высокая	CVE-2026-3902	Ubuntu	Сетевой	SB	2026-06-02	✓
16	Высокая	CVE-2026-44705	node-tmp	Сетевой	OSI	2026-06-03	✓
17	Высокая	CVE-2026-10292	UTT HiPER 1200GW	Сетевой	DoS	2026-06-02	✓
18	Высокая	CVE-2026-26001	GLPI Inventory	Сетевой	ACE	2026-05-28	✓
19	Высокая	CVE-2026-44492	axios	Сетевой	SB	2026-06-03	✓
20	Высокая	CVE-2026-10293	UTT HiPER 1250GW	Сетевой	DoS	2026-06-02	✓
21	Критическая	CVE-2026-41104	Microsoft Planetary Computer Pro	Сетевой	OSI	2026-05-26	✓
22	Критическая	CVE-2026-47280	Azure Resource Manager	Сетевой	PE	2026-05-26	✓
23	Критическая	CVE-2026-40412	Azure Orbital Spatio	Сетевой	ACE	2026-05-26	✓
24	Критическая	CVE-2026-42901	Microsoft Entra ID	Сетевой	PE	2026-05-26	✓
25	Критическая	CVE-2026-23652	Microsoft Power Pages	Сетевой	ACE	2026-05-26	✓
26	Критическая	CVE-2026-41615	Authenticator	Сетевой	OSI	2020-07-03	✓
27	Критическая	CVE-2026-33843	Microsoft Entra ID	Сетевой	PE	2026-05-27	✓
28	Высокая	CVE-2026-23663	Microsoft Entra ID	Сетевой	PE	2026-05-27	✓

29	Высокая	CVE-2026-45659	Microsoft SharePoint Server	Сетевой	ACE	2026-05-27	✓
30	Критическая	CVE-2026-40411	Azure Virtual Network Gateway	Сетевой	ACE	2026-05-27	✓
31	Критическая	CVE-2026-44494	axios	Сетевой	OSI	2026-06-03	✓
32	Критическая	CVE-2026-34908	UniFi OS Server	Сетевой	ACE	2026-06-02	✓
33	Высокая	CVE-2026-34911	UniFi OS Server	Сетевой	OSI	2026-06-02	✓
34	Критическая	CVE-2026-33000	UniFi OS Server	Сетевой	ACE	2026-06-02	✓
35	Критическая	CVE-2026-10064	TRENDnet TEW-432BRP	Сетевой	ACE	2026-06-04	✓
36	Критическая	CVE-2026-10060	TRENDnet TEW-432BRP	Сетевой	ACE	2026-06-04	✓
37	Критическая	CVE-2026-34909	UniFi OS Server	Сетевой	OSI	2026-06-02	✓
38	Критическая	CVE-2026-10061	TRENDnet TEW-432BRP	Сетевой	ACE	2026-06-04	✓
39	Критическая	CVE-2026-34910	UniFi OS Server	Сетевой	ACE	2026-06-02	✓
40	Высокая	CVE-2026-7504	Keycloak	Сетевой	OSI	2026-06-04	✓
41	Высокая	BDU:2026-07797	libinput	Локальный	ACE	2026-06-04	✓
42	Высокая	CVE-2026-10270	DI-7001 MINI	Сетевой	DoS	2026-06-04	✓
43	Высокая	CVE-2026-20230	Cisco Unified Communications Manager	Сетевой	RLF	2026-06-04	✓

44	Высокая	CVE-2026-43023	Linux	Локальный	DoS	2026-05-06	✓
45	Высокая	CVE-2026-43056	Linux	Локальный	DoS	2026-05-06	✓
46	Высокая	CVE-2026-43050	Linux	Смежная сеть	DoS	2026-05-06	✓
47	Высокая	CVE-2026-43020	Linux	Локальный	DoS	2026-05-12	✓
48	Критическая	CVE-2026-43039	Linux	Сетевой	DoS	2026-05-14	✓
49	Критическая	CVE-2026-43037	Linux	Сетевой	ACE	2026-05-14	✓
50	Высокая	CVE-2026-28476	OpenClaw	Сетевой	RLF	2026-04-22	✓
51	Высокая	CVE-2026-28473	OpenClaw	Сетевой	SB	2026-04-22	✓
52	Высокая	CVE-2026-9312	GitHub Enterprise Server	Сетевой	OSI	2026-06-01	✓
53	Высокая	CVE-2026-31944	LibreChat	Сетевой	OSI	2026-03-27	✓
54	Высокая	CVE-2026-28477	OpenClaw	Сетевой	LoI	2026-04-22	✓
55	Высокая	CVE-2026-4276	LibreChat	Сетевой	LoI	2026-03-27	✓
56	Высокая	CVE-2026-33811	Go	Сетевой	DoS	2026-06-08	✓
57	Высокая	CVE-2026-39836	Go	Сетевой	DoS	2026-06-08	✓
58	Высокая	CVE-2026-22909	SICK TDC-X401GL	Сетевой	DoS	2026-01-16	✓

59	Высокая	CVE-2026-39820	Go	Сетевой	DoS	2026-06-08	✓
60	Высокая	CVE-2026-42499	Go	Сетевой	DoS	2026-06-08	✓
61	Критическая	CVE-2026-25293	QCA7005	Смежная сеть	ACE	2026-05-07	✓
62	Высокая	CVE-2026-20245	Catalyst SD-WAN Manager	Локальный	ACE	2026-06-08	✓
63	Высокая	CVE-2026-10878	DWR-M920	Сетевой	ACE	2026-06-08	✓
64	Критическая	CVE-2026-2651	MLflow	Сетевой	ACE	2026-06-08	✓
65	Высокая	CVE-2026-28318	SolarWinds Serv-U	Сетевой	DoS	2026-06-08	✓
66	Критическая	CVE-2026-6942	radare2-mcp	Сетевой	ACE	2026-06-08	✓
67	Критическая	CVE-2026-39179	Sogo	Сетевой	ACE	2026-06-04	✓
68	Критическая	CVE-2026-39178	Sogo	Сетевой	ACE	2026-06-04	✓
69	Высокая	CVE-2026-34040	Moby Project	Локальный	PE	2026-05-02	✓
70	Критическая	CVE-2026-3381	zlib	Сетевой	ACE	2026-05-28	✓
71	Высокая	CVE-2025-8850	LibreChat	Сетевой	LoI	2026-03-16	✓
72	Высокая	CVE-2026-23406	Linux	Локальный	ACE	2026-04-07	✓
73	Высокая	CVE-2026-23408	Linux	Локальный	ACE	2026-04-07	✓

74	Критическая	CVE-2026-4670	MOVEit Automation	Сетевой	PE	2026-05-12	✓
75	Высокая	CVE-2026-41882	IntelliJ IDEA	Сетевой	OSI	2026-05-07	✓
76	Критическая	CVE-2026-25254	QSC	Сетевой	ACE	2026-05-07	✓
77	Высокая	CVE-2026-25255	QSC	Локальный	PE	2026-05-07	✓
78	Высокая	CVE-2026-45109	Next.js	Сетевой	OSI	2026-05-15	✓

1

Краткое описание: Отказ в обслуживании в Microsoft Teams for Android

Идентификатор уязвимости: CVE-2026-42835

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: Microsoft Teams for Android: до 1.0.76.2026111302

Категория уязвимого продукта: Мобильные платформы

Способ эксплуатации: Некорректная нейтрализация специальных элементов.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42835

2

Краткое описание: Выполнение произвольного кода в FortiSandbox

Идентификатор уязвимости: CVE-2026-25089

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

Уязвимый продукт: FortiSandbox: 4.4.0 - 5.0.5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Некорректная нейтрализация специальных элементов.

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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-26-141

3

Краткое описание: Выполнение произвольного кода в SAP NetWeaver Application Server Java Web Container

Идентификатор уязвимости: CVE-2026-40128

Идентификатор программной ошибки: CWE-35 Выход за пределы каталога с помощью [1.ков.].../...//[1.ков.]

Уязвимый продукт: SAP NetWeaver AS JAVA: 7.50

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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.

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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://me.sap.com/notes/3727078
- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2026.html

4

Краткое описание: Получение конфиденциальной информации в TP-Link products

Идентификатор уязвимости: CVE-2026-34126

Идентификатор программной ошибки: CWE-319 Передача важных данных в незашифрованном виде

Уязвимый продукт: Tapo D100C: до 1.3.1 260421 Rel.031658
Tapo P300: до 1.4.0 260416 Rel.014037, 1.4.2 251219 Rel.142654
Tapo L535E: до 1.4.1 251016 Rel.204554

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: 7.0 AV:A/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://jvn.jp/en/jp/JVN70631953/index.html
- https://www.tp-link.com/us/support/faq/5106/

5

Краткое описание: Повышение привилегий в Apache Solr

Идентификатор уязвимости: CVE-2026-44825

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: Apache Solr: 9.4.0 - 10.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Использование жестко закодированных учетных данных

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: 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: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://lists.apache.org/api/email.lua?id=vc20fkov1g9ckg5oco8y87wxyh6ysq64
- https://issues.apache.org/jira/browse/SOLR-18233

6

Краткое описание: Отказ в обслуживании в Microsoft IIS HTTP/2 support

Идентификатор уязвимости: CVE-2026-49975

Идентификатор программной ошибки: CWE-789 Неконтролируемое выделение памяти

Уязвимый продукт: Microsoft Internet Information Services (IIS): 10.0, 10.0.08608

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

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: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://blog.calif.io/p/codex-discovered-a-hidden-http2-bomb
- https://github.com/califio/publications/tree/main/MADBugs/http2-bomb

Краткое описание: Обход безопасности в Linux kernel netfilter

Идентификатор уязвимости: CVE-2026-46244

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Linux kernel: 7.0 rc1, 7.0 rc2

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://git.kernel.org/stable/c/689bbf48c1f45130086ae1c46ab83ea4c753c601
- https://git.kernel.org/stable/c/870d59e2cf218e7418491e26bad768cb16654582
- https://git.kernel.org/stable/c/b6a91f68ebfed9c38e0e9150f58a9b85da07181c
- https://git.kernel.org/stable/c/c161ad9157f5a0429b5ff94d9770faf3bf48d273
- https://git.kernel.org/stable/c/d0f98a3617f6ae5b1e95cde1e68e7ead4a1279ce

Краткое описание: Выполнение произвольного кода в Mirasvit Cache Warmer for Magento 2

Идентификатор уязвимости: CVE-2026-45247

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Full Page Cache Warmer for Magento 2: 1.0.1 - 1.11.11

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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.

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

Оценка CVSSv4: 9.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://mirasvit.com/package/changelog/?package=mirasvit/module-cache-warmer
- https://sansec.io/research/mirasvit-cache-warmer-object-injection
- https://www.vulncheck.com/advisories/mirasvit-cache-warmer-for-magento-php-object-injection
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-45247
- https://www.imperva.com/blog/imperva-customers-protected-against-cve-2026-45247-in-mirasvit-full-page-cache-warmer-for-magento/

Краткое описание: Обход безопасности в Linux kernel ipv6

Идентификатор уязвимости: CVE-2026-46266

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Linux kernel: 7.0 rc1, 7.0 rc2

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

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Обход безопасности

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.

9

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://git.kernel.org/stable/c/19e42490c89bac9a388f28179e66bebbef350f99
- https://git.kernel.org/stable/c/531c1aec81bfe19d00af13da5531fbb8209e4bd2
- https://git.kernel.org/stable/c/719d3932b8f6e3348ce2f0ac58e278301fc17575
- https://git.kernel.org/stable/c/c89477ad7944867394360b29bb801010fc3ff22
- https://git.kernel.org/stable/c/db76b75ede3810e7cf9cfea5067d4f3e0993768b

Краткое описание: Выполнение произвольного кода в GLPI Project

Идентификатор уязвимости: CVE-2026-25936
BDU:2026-07741

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

Уязвимый продукт: РЕД ОС: 8.0
GLPI: от 11.0.0 до 11.0.6

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

10 **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: 2026-05-28 / 2026-05-28

Ссылки на источник:

- https://github.com/glpi-project/glpi/security/advisories/GHSA-qw3x-7vv2-7759
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-25936
- https://bdu.fstec.ru/vul/2026-07741

Краткое описание: Выполнение произвольного кода в Firebird

Идентификатор уязвимости: CVE-2026-40342
BDU:2026-07740

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

Уязвимый продукт: Firebird: до 3.0.14
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

11 **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: 9.9 AV:N/AC:L/PR:L/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: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://github.com/FirebirdSQL/firebird/security/advisories/GHSA-7pxc-h3rv-r257
- https://redos.red-soft.ru/search/?q=CVE-2026-40342
- https://bdu.fstec.ru/vul/2026-07740

12

Краткое описание: Отказ в обслуживании в Django

Идентификатор уязвимости: CVE-2026-25673
BDU:2026-07737

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

Уязвимый продукт: Django: от 4.2 до 4.2.29
РЕД ОС: 8.0

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.

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: 2026-05-28 / 2026-05-28

Ссылки на источник:

- https://github.com/django/django
- https://groups.google.com/g/django-announce
- https://github.com/advisories/GHSA-8p8v-wh79-9r56
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-25673
- https://docs.djangoproject.com/en/dev/releases/security/
- https://github.com/django/django/commit/b1444d9acf43db9de96e0da2b4737ad56af0eb76
- https://github.com/django/django/commit/4d3c184686626d224d9a87451410ecf802b41f7c
- https://github.com/django/django/commit/b3e8ec8cc310489fe80174b14b11edb970d682ea
- https://bdu.fstec.ru/vul/2026-07737

Краткое описание: Отказ в обслуживании в Ubuntu

Идентификатор уязвимости: CVE-2026-33034
BDU:2026-07725

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Ubuntu: 25.10
Django: от 6.0 до 6.0.4
РЕД ОС: 8.0

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.

13 **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: 2026-05-28 / 2026-05-28

Ссылки на источник:

- https://www.djangoproject.com/weblog/2026/apr/07/security-releases/
- https://github.com/django/django/commit/953c238058c0ce387a1a41cb491bfc1875d73ad0
- https://github.com/django/django/commit/393dbc53e848876fdba92fbf02e10ee6a6eace6b
- https://github.com/django/django/commit/49e1e2b548999a35a025f9682598946bda9e9921
- https://github.com/django/django/commit/ed4dfda62718a0bb644b80ac8b1d3099861f2295
- https://groups.google.com/g/django-announce
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-33034
- https://ubuntu.com/security/CVE-2026-33034
- https://bdu.fstec.ru/vul/2026-07725

14

Краткое описание: Получение конфиденциальной информации в Ubuntu

Идентификатор уязвимости: CVE-2026-4277
BDU:2026-07723

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Ubuntu: 25.10
Django: от 6.0 до 6.0.4
Red Hat Satellite: 6
РЕД ОС: 8.0
Ansible Automation Platform: 2
Discovery: 2

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

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: 2026-06-03 / 2026-06-03

Ссылки на источник:

- https://groups.google.com/g/django-announce
- https://www.djangoproject.com/weblog/2026/apr/07/security-releases/
- https://docs.djangoproject.com/en/dev/releases/security/
- https://github.com/django/django
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-4277
- https://ubuntu.com/security/CVE-2026-4277

- https://access.redhat.com/security/cve/cve-2026-4277
- https://bdu.fstec.ru/vul/2026-07723

15

Краткое описание: Обход безопасности в Ubuntu

Идентификатор уязвимости: CVE-2026-3902
BDU:2026-07722

Идентификатор программной ошибки: CWE-290 Обход аутентификации, связанный с подменой данных

Уязвимый продукт: Ubuntu: 25.10
Django: от 6.0 до 6.0.4
Red Hat Satellite: 6
РЕД ОС: 8.0
Ansible Automation Platform: 2
Discovery: 2

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

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Обход безопасности

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:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-02 / 2026-06-02

Ссылки на источник:

- https://groups.google.com/g/django-announce
- https://www.djangoproject.com/weblog/2026/apr/07/security-releases/
- https://docs.djangoproject.com/en/dev/releases/security/
- https://redos.red-soft.ru/search/?iblock_id=&q=cve-2026-3902
- https://access.redhat.com/security/cve/cve-2026-3902
- https://ubuntu.com/security/CVE-2026-3902

- https://bdu.fstec.ru/vul/2026-07722

16

Краткое описание: Получение конфиденциальной информации в node-tmp

Идентификатор уязвимости: CVE-2026-44705
BDU:2026-07719

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

Уязвимый продукт: node-tmp: до 0.2.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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://github.com/raszi/node-tmp/security/advisories/GHSA-ph9p-34f9-6g65/#poc
- https://bdu.fstec.ru/vul/2026-07719

17

Краткое описание: Отказ в обслуживании в UTT HiPER 1200GW

Идентификатор уязвимости: CVE-2026-10292
BDU:2026-07712

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: UTT HiPER 1200GW: до 2.5.3-170306 включительно

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: 2026-06-02 / 2026-06-02

Ссылки на источник:

- https://github.com/yuezhaoshanmu/cve/blob/main/1.md
- https://bdu.fstec.ru/vul/2026-07712

18

Краткое описание: Выполнение произвольного кода в GLPI Inventory

Идентификатор уязвимости: CVE-2026-26001
BDU:2026-07742

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

Уязвимый продукт: РЕД ОС: 8.0
GLPI Inventory: до 1.6.5

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: 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: 2026-05-28 / 2026-05-28

Ссылки на источник:

- https://github.com/glpi-project/glpi-inventory-plugin/security/advisories/GHSA-gp4r-m42c-wvgx
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-26001
- https://bdu.fstec.ru/vul/2026-07742

19

Краткое описание: Обход безопасности в axios

Идентификатор уязвимости: CVE-2026-44492
BDU:2026-07710

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

Уязвимый продукт: axios: от 0.31.1 до 0.32.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Обход безопасности

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:N/AC:L/PR:N/UI:N/S:C/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://github.com/twentyhq/twenty/issues/21071
- https://github.com/axios/axios/security/advisories/GHSA-pjwm-pj3p-43mv/#poc
- https://bdu.fstec.ru/vul/2026-07710

Краткое описание: Отказ в обслуживании в UTT HiPER 1250GW

Идентификатор уязвимости: CVE-2026-10293
BDU:2026-07711

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: UTT HiPER 1250GW: до 3.2.7-210907-180535 включительно

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

20 **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: 2026-06-02 / 2026-06-02

Ссылки на источник:

- https://github.com/yuezhaoshanmu/cve/blob/main/2.md
- https://bdu.fstec.ru/vul/2026-07711

Краткое описание: Получение конфиденциальной информации в Microsoft Planetary Computer Pro

Идентификатор уязвимости: CVE-2026-41104
BDU:2026-07696

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft Planetary Computer Pro: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Получение конфиденциальной информации

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: 10.0 AV:N/AC:L/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: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41104
- https://bdu.fstec.ru/vul/2026-07696

Краткое описание: Повышение привилегий в Azure Resource Manager

Идентификатор уязвимости: CVE-2026-47280
BDU:2026-07697

Идентификатор программной ошибки: CWE-289 Обход аутентификации, связанный с альтернативными именами

Уязвимый продукт: Azure Resource Manager: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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: 10.0 AV:N/AC:L/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: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47280
- https://bdu.fstec.ru/vul/2026-07697

Краткое описание: Выполнение произвольного кода в Azure Orbital Spatio

Идентификатор уязвимости: CVE-2026-40412
BDU:2026-07698

Идентификатор программной ошибки: CWE-434 Отсутствие ограничений на загрузку файлов небезопасного типа

Уязвимый продукт: Azure Orbital Spatio: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Выполнение произвольного кода

23 **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: 10.0 AV:N/AC:L/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: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40412
- https://bdu.fstec.ru/vul/2026-07698

Краткое описание: Повышение привилегий в Microsoft Entra ID

Идентификатор уязвимости: CVE-2026-42901
BDU:2026-07699

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

Уязвимый продукт: Microsoft Entra ID: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Повышение привилегий

24 **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: 10.0 AV:N/AC:L/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: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42901
- https://bdu.fstec.ru/vul/2026-07699

Краткое описание: Выполнение произвольного кода в Microsoft Power Pages

Идентификатор уязвимости: CVE-2026-23652
BDU:2026-07700

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

Уязвимый продукт: Microsoft Power Pages: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

25

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: 10.0 AV:N/AC:L/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: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-23652
- https://bdu.fstec.ru/vul/2026-07700

26

Краткое описание: Получение конфиденциальной информации в Authenticator

Идентификатор уязвимости: CVE-2026-41615
BDU:2026-07694

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

Уязвимый продукт: Authenticator: до 6.2605.2973

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2020-07-03 / 2020-07-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41615
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-40974
- https://bdu.fstec.ru/vul/2026-07694

27

Краткое описание: Повышение привилегий в Microsoft Entra ID

Идентификатор уязвимости: CVE-2026-33843
BDU:2026-07702

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

Уязвимый продукт: Microsoft Entra ID: -

Категория уязвимого продукта: Операционные системы Microsoft 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.

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

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33843
- https://bdu.fstec.ru/vul/2026-07702

Краткое описание: Повышение привилегий в Microsoft Entra ID

Идентификатор уязвимости: CVE-2026-23663
BDU:2026-07704

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Microsoft Entra ID: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

28 **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: 2026-05-27 / 2026-05-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-23663
- https://bdu.fstec.ru/vul/2026-07704

29

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2026-45659
BDU:2026-07705

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft SharePoint Server: 2019
Microsoft SharePoint Server Subscription Edition: -
Microsoft SharePoint Enterprise Server 2016: -

Категория уязвимого продукта: Операционные системы Microsoft и их 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.

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45659
- https://todayincyber.io/feed/malware/article/019e7d1f-bf4d-794c-84a4-8affd49f3cdf
- https://bdu.fstec.ru/vul/2026-07705

Краткое описание: Выполнение произвольного кода в Azure Virtual Network Gateway

Идентификатор уязвимости: CVE-2026-40411
BDU:2026-07701

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Azure Virtual Network Gateway: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

30 **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: 9.9 AV:N/AC:L/PR:L/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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40411
- https://bdu.fstec.ru/vul/2026-07701

31

Краткое описание: Получение конфиденциальной информации в axios

Идентификатор уязвимости: CVE-2026-44494
BDU:2026-07709

Идентификатор программной ошибки: CWE-1008 Архитектурные принципы

Уязвимый продукт: axios: от 1.0.0 до 1.16.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

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://github.com/axios/axios
- https://github.com/axios/axios/security/advisories/GHSA-35jp-ww65-95wh/#poc
- https://bdu.fstec.ru/vul/2026-07709

32

Краткое описание: Выполнение произвольного кода в UniFi OS Server

Идентификатор уязвимости: CVE-2026-34908
BDU:2026-07800

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: UniFi OS Server: до 5.0.6 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

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: 10.0 AV:N/AC:L/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: 2026-06-02 / 2026-06-02

Ссылки на источник:

- https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
- https://github.com/advisories/GHSA-p8c5-xwrc-584f
- https://bdu.fstec.ru/vul/2026-07800

33

Краткое описание: Получение конфиденциальной информации в UniFi OS Server

Идентификатор уязвимости: CVE-2026-34911
BDU:2026-07801

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

Уязвимый продукт: UniFi OS Server: до 5.0.6 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-02 / 2026-06-02

Ссылки на источник:

- https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
- https://bdu.fstec.ru/vul/2026-07801

Краткое описание: Выполнение произвольного кода в UniFi OS Server

Идентификатор уязвимости: CVE-2026-33000
BDU:2026-07802

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: UniFi OS Server: до 5.0.6 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

34 **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: 2026-06-02 / 2026-06-02

Ссылки на источник:

- https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
- https://bdu.fstec.ru/vul/2026-07802

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

Идентификатор уязвимости: CVE-2026-10064
BDU:2026-07803

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.

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: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://github.com/wudipjq/my_vuln/blob/main/TRENDnet/vuln_5/5.md
- https://bdu.fstec.ru/vul/2026-07803

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

Идентификатор уязвимости: CVE-2026-10060
BDU:2026-07804

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

Уязвимый продукт: TRENDnet TEW-432BRP: 3.10B20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

36

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: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://github.com/wudipjq/my_vuln/blob/main/TRENDnet/vuln_1/1.md
- https://bdu.fstec.ru/vul/2026-07804

37

Краткое описание: Получение конфиденциальной информации в UniFi OS Server

Идентификатор уязвимости: CVE-2026-34909
BDU:2026-07799

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

Уязвимый продукт: UniFi OS Server: до 5.0.6 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 10.0 AV:N/AC:L/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: 2026-06-02 / 2026-06-02

Ссылки на источник:

- https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
- https://github.com/advisories/GHSA-95fp-244g-g3vr
- https://bdu.fstec.ru/vul/2026-07799

38

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

Идентификатор уязвимости: CVE-2026-10061
BDU:2026-07805

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

Уязвимый продукт: TRENDnet TEW-432BRP: 3.10B20

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: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://github.com/wudipjq/my_vuln/blob/main/TRENDnet/vuln_2/2.md
- https://bdu.fstec.ru/vul/2026-07805

Краткое описание: Выполнение произвольного кода в UniFi OS Server

Идентификатор уязвимости: CVE-2026-34910
BDU:2026-07798

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: UniFi OS Server: до 5.0.6 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

39 **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: 10.0 AV:N/AC:L/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: 2026-06-02 / 2026-06-02

Ссылки на источник:

- https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
- https://bdu.fstec.ru/vul/2026-07798

Краткое описание: Получение конфиденциальной информации в Keycloak

Идентификатор уязвимости: CVE-2026-7504
BDU:2026-07782

Идентификатор программной ошибки: CWE-601 Перенаправление на небезопасный сайт ("открытое перенаправление")

Уязвимый продукт: Keycloak: до 26.7.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

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.

40

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://www.keycloak.org/2026/05/keycloak-2662-released
- https://github.com/keycloak/keycloak/issues/49109
- https://github.com/advisories/GHSA-rp95-xpg9-c2cq
- https://access.redhat.com/security/cve/cve-2026-7504
- https://dailycve.com/keycloak-open-redirect-bypass-cve-2026-7504-high-dc-jun2026-162/
- https://bdu.fstec.ru/vul/2026-07782

Краткое описание: Выполнение произвольного кода в libinput

Идентификатор уязвимости: BDU:2026-07797

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

Уязвимый продукт: libinput: до 1.30.3 включительно

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.

41

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: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://gitlab.freedesktop.org/libinput/libinput/-/releases/1.30.4
- https://gitlab.freedesktop.org/libinput/libinput/-/releases/1.31.3
- https://lore.freedesktop.org/wayland-devel/aiDRA35Gggyi5mTY@quokka/
- https://gitlab.freedesktop.org/libinput/libinput/-/work_items/1296
- https://bdu.fstec.ru/vul/2026-07797

42

Краткое описание: Отказ в обслуживании в DI-7001 MINI

Идентификатор уязвимости: CVE-2026-10270
BDU:2026-07781

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DI-7001 MINI: до 19.09.19A1 включительно

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://github.com/666324/dlink-DI-7001MINI-8G-vuln
- https://github.com/666324/dlink-DI-7001MINI-8G-vuln/tree/main/dlink-DI-7001MINI-8G-vuln
- https://bdu.fstec.ru/vul/2026-07781

Краткое описание: Чтение локальных файлов в Cisco Unified Communications Manager

Идентификатор уязвимости: CVE-2026-20230
BDU:2026-07815

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

Уязвимый продукт: Cisco Unified Communications Manager: от 15 до 15SU5
Cisco Unified Communications Manager SME: от 15 до 15SU5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Чтение локальных файлов

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW
- https://undercodenews.com/cve-2026-20230-critical-cisco-unified-cm-ssrf-flaw-exposes-enterprises-to-root-level-takeover-via-public-exploit-code-video/
- https://www.acn.gov.it/portale/w/cisco-cucm-disponibile-poc-per-lo-sfruttamento-di-vulnerabilita
- https://bdu.fstec.ru/vul/2026-07815

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43023
BDU:2026-07837

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 6.19 до 6.19.12
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование сроками и состоянием.

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:** 7.8 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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026050158-CVE-2026-43023-19eb@gregkh/
- https://git.kernel.org/stable/c/dabf22269242e2f2bf44c43fcdc2fa763df7f9cc
- https://git.kernel.org/stable/c/adb90cd0f9f7a8d438fcb93354040fbafc5ae2a0
- https://git.kernel.org/stable/c/7e296ffdab5bdab718dff7c14288fdcb9154fa27
- https://git.kernel.org/stable/c/98c8d3bfdaa657d8f472dbbebd7ea8cd816d8a8d
- https://git.kernel.org/stable/c/d002bd11024bd231bcb606877e33951ffb7bed14
- https://git.kernel.org/stable/c/8a5b0135d4a5d9683203a3d9a12a711ccec5936b
- https://access.redhat.com/security/cve/cve-2026-43023
- https://security-tracker.debian.org/tracker/CVE-2026-43023

- https://feedly.com/cve/CVE-2026-43023
- https://bdu.fstec.ru/vul/2026-07837

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43056
BDU:2026-07836

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.2 до 6.6.134
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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

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.

45 **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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026050108-CVE-2026-43056-fefd@gregkh/
- https://git.kernel.org/stable/c/43f5b19fd190fea20d052bc84741b28031d5baa9
- https://git.kernel.org/stable/c/5f4061f8225d18695e5afe9bbf1cb7bd673d7872
- https://git.kernel.org/stable/c/c4ea7d8907cf72b259bf70bd8c2e791e1c4ff70f
- https://git.kernel.org/stable/c/d88541ffd56d62a61e77209080001eddd4d69815
- https://git.kernel.org/stable/c/e5a75bf026c686b91a7dc6f9c5caf5016745d1fe
- https://security-tracker.debian.org/tracker/CVE-2026-43056
- https://access.redhat.com/security/cve/cve-2026-43056
- https://bdu.fstec.ru/vul/2026-07836

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43050
BDU:2026-07835

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: до 5.10.253
Red Hat Enterprise Linux: 9
Debian GNU/Linux: 13

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

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.

46 **Оценка CVSSv3:** 8.0 AV:A/AC:L/PR:L/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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026050106-CVE-2026-43050-1cd2@gregkh/
- https://git.kernel.org/stable/c/317843d5355062020649124eb4a0d7acbcc3f53e
- https://git.kernel.org/stable/c/3989740fa4978e1d2d51ecc62be1b01093e104ad
- https://git.kernel.org/stable/c/3e8b25f32f2f35549d03d77da030a24a45bdef5b
- https://git.kernel.org/stable/c/5fbbb1ff936d7ff9528d929c1549977e8123d8a8
- https://git.kernel.org/stable/c/750a33f417f3d196b86375f8d9f8938bacf130fe
- https://git.kernel.org/stable/c/922814879542c2e397b0e9641fd36b8202a8e555
- https://git.kernel.org/stable/c/abc10f85a3965ac14b9ed7ad3e67b35604a63aa3
- https://git.kernel.org/stable/c/b256d055da47258e63f8b40965f276c5f23d229a

- https://security-tracker.debian.org/tracker/CVE-2026-43050
- https://access.redhat.com/security/cve/cve-2026-43050
- https://bdu.fstec.ru/vul/2026-07835

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43020
BDU:2026-07834

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 3.4 до 5.10.253
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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

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.

47 **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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026050157-CVE-2026-43020-3561@gregkh/
- https://git.kernel.org/stable/c/0f37d1e65c6d71ad94ccfb5c602163c525db789d
- https://git.kernel.org/stable/c/257cdb960d8ff6d60bb6461b03c814b6cf0c9e64
- https://git.kernel.org/stable/c/40ba329e8b4cd2fb11b0caf5e6a543ceaebb6009
- https://git.kernel.org/stable/c/50fb64defa72a3fecd0af1ca7c6b47b5c5c2b257
- https://git.kernel.org/stable/c/82f342b3b006ca1d65f4890c05f2ec32fcb808b6
- https://git.kernel.org/stable/c/b8dbe9648d69059cfe3a28917bfbf7e61efd7f15
- https://git.kernel.org/stable/c/c34577f517b556fb6ca173d45bf7e766ae2564ce
- https://git.kernel.org/stable/c/f71695e81f4cb428f3c7e2138eae88199005b52c

- https://security-tracker.debian.org/tracker/CVE-2026-43020
- https://access.redhat.com/security/cve/cve-2026-43020
- https://bdu.fstec.ru/vul/2026-07834

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43039
BDU:2026-07833

Идентификатор программной ошибки: CWE-909 Отсутствует инициализация ресурса

Уязвимый продукт: Linux: от 6.19 до 6.19.12

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.

48

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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://git.kernel.org/stable/c/5597dd284ff8c556c0b00f6a34473677426e3f81
- https://git.kernel.org/stable/c/a968438d4fc17ee1dcdc3cfa490dcb5e7709cf76
- https://lore.kernel.org/linux-cve-announce/2026050103-CVE-2026-43039-ff5c@gregkh/
- https://bdu.fstec.ru/vul/2026-07833

49

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43037
BDU:2026-07832

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 2.6.22 до 5.10.253
Red Hat Enterprise Linux: 9.6 Extended Update Support
Ubuntu: 25.10
Debian GNU/Linux: 13
АЛЬТ СП 10: -

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

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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://git.kernel.org/stable/c/1063515ce15ff31065c4e7f8265f4c2fd3c54876
- https://git.kernel.org/stable/c/2cc6e3b0fe0f0242d1f530a93a4924f48ab85ba5
- https://git.kernel.org/stable/c/2edfa31769a4add828a7e604b21cb82aaaa05925
- https://git.kernel.org/stable/c/4a622658f384b03560834cbe8ffcfe69a278f7c8
- https://git.kernel.org/stable/c/590f622669b97eaf7b57a1de7b0a6e68c5d8b2c3
- https://git.kernel.org/stable/c/a0c4ce9900a108eaf55d0f3b399cb55999647d39
- https://git.kernel.org/stable/c/d6621f60192fe10c047a4487be42a6f4c150707f

- https://git.kernel.org/stable/c/ea9f65b27c8404e164848ebff1443310fd187629
- https://lore.kernel.org/linux-cve-announce/2026050102-CVE-2026-43037-0346@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43037
- https://access.redhat.com/security/cve/cve-2026-43037
- https://ubuntu.com/security/CVE-2026-43037
- https://cve.basealt.ru/
- https://bdu.fstec.ru/vul/2026-07832

Краткое описание: Чтение локальных файлов в OpenClaw

Идентификатор уязвимости: CVE-2026-28476
BDU:2026-07918

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

Уязвимый продукт: OpenClaw: до 2026.2.14

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Чтение локальных файлов

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: 8.3 AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://github.com/openclaw/openclaw/security/advisories/GHSA-pg2v-8xwh-qhcc
- https://github.com/openclaw/openclaw/commit/bfa7d21e997baa8e3437657d59b1e296815cc1b1
- https://www.vulncheck.com/advisories/openclaw-server-side-request-forgery-in-tlon-extension-authentication
- https://bdu.fstec.ru/vul/2026-07918

Краткое описание: Обход безопасности в OpenClaw

Идентификатор уязвимости: CVE-2026-28473
BDU:2026-07917

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: OpenClaw: до 2026.2.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://github.com/openclaw/openclaw/security/advisories/GHSA-mqpw-46fh-299h
- https://github.com/openclaw/openclaw/commit/efe2a464afcff55bb5a95b959e6bd9ec0fef086e
- https://www.vulncheck.com/advisories/openclaw-authorization-bypass-via-approve-chat-command
- https://bdu.fstec.ru/vul/2026-07917

Краткое описание: Получение конфиденциальной информации в GitHub Enterprise Server

Идентификатор уязвимости: CVE-2026-9312
BDU:2026-07906

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

Уязвимый продукт: GitHub Enterprise Server: до 3.21.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

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.

52 **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: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://docs.github.com/en/enterprise-server@3.16/admin/release-notes#3.16.20
- https://docs.github.com/en/enterprise-server@3.17/admin/release-notes#3.17.17
- https://docs.github.com/en/enterprise-server@3.18/admin/release-notes#3.18.11
- https://docs.github.com/en/enterprise-server@3.19/admin/release-notes#3.19.8
- https://docs.github.com/en/enterprise-server@3.20/admin/release-notes#3.20.4
- https://docs.github.com/en/enterprise-server@3.21/admin/release-notes#3.21.1
- https://bdu.fstec.ru/vul/2026-07906

Краткое описание: Получение конфиденциальной информации в LibreChat

Идентификатор уязвимости: CVE-2026-31944
BDU:2026-07911

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

Уязвимый продукт: LibreChat: от 0.8.2 до 0.8.2-rc3 (включительно)

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.

53

Оценка CVSSv3: 7.6 AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-27 / 2026-03-27

Ссылки на источник:

- https://github.com/danny-avila/LibreChat/security/advisories/GHSA-vf7j-7mrx-hp7g
- https://bdu.fstec.ru/vul/2026-07911

Краткое описание: Потеря целостности в OpenClaw

Идентификатор уязвимости: CVE-2026-28477
BDU:2026-07920

Идентификатор программной ошибки: CWE-352 Подделка межсайтового запроса (CSRF)

Уязвимый продукт: OpenClaw: до 2026.2.14

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Потеря целостности

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.

54

Оценка CVSSv3: 8.3 AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://github.com/openclaw/openclaw/security/advisories/GHSA-7rcp-mxpq-72pj
- https://github.com/openclaw/openclaw/commit/a99ad11a4107ba8eac58f54a3c1a8a0cf5686f47
- https://www.vulncheck.com/advisories/openclaw-oauth-state-validation-bypass-in-manual-chutes-login-flow
- https://bdu.fstec.ru/vul/2026-07920

55

Краткое описание: Потеря целостности в LibreChat

Идентификатор уязвимости: CVE-2026-4276
BDU:2026-07913

Идентификатор программной ошибки: CWE-117 Некорректная нейтрализация выходных данных для записи в журналы

Уязвимый продукт: LibreChat: 0.7.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Потеря целостности

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:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-27 / 2026-03-27

Ссылки на источник:

- https://kb.cert.org/vuls/id/624941
- https://www.kb.cert.org/vuls/id/624941
- https://bdu.fstec.ru/vul/2026-07913

56

Краткое описание: Отказ в обслуживании в Go

Идентификатор уязвимости: CVE-2026-33811
BDU:2026-07950

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Go: от 1.26.0 до 1.26.3

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: 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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://go.dev/cl/767860
- https://go.dev/issue/78803
- https://groups.google.com/g/golang-announce/c/qcCIEXso47M
- https://pkg.go.dev/vuln/GO-2026-4981
- https://bdu.fstec.ru/vul/2026-07950

Краткое описание: Отказ в обслуживании в Go

Идентификатор уязвимости: CVE-2026-39836
BDU:2026-07949

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Go: от 1.26.0 до 1.26.3

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.

57

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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://pkg.go.dev/vuln/GO-2026-4971
- https://go-review.googlesource.com/c/go/+/775320
- https://github.com/golang/go/issues/79006
- https://github.com/golang/go/issues/79028
- https://bdu.fstec.ru/vul/2026-07949

58

Краткое описание: Отказ в обслуживании в SICK TDC-X401GL

Идентификатор уязвимости: CVE-2026-22909
BDU:2026-07900

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: SICK TDC-X401GL: -

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Нарушение авторизации.

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: 2026-01-16 / 2026-01-16

Ссылки на источник:

- https://www.sick.com/.well-known/csaf/white/2026/sca-2026-0001.pdf
- https://bdu.fstec.ru/vul/2026-07900

Краткое описание: Отказ в обслуживании в Go

Идентификатор уязвимости: CVE-2026-39820
BDU:2026-07953

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Go: от 1.26.0 до 1.26.3

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.

59

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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://go.dev/cl/759940
- https://go.dev/issue/78566
- https://groups.google.com/g/golang-announce/c/qcCIEXso47M
- https://pkg.go.dev/vuln/GO-2026-4986
- https://bdu.fstec.ru/vul/2026-07953

60

Краткое описание: Отказ в обслуживании в Go

Идентификатор уязвимости: CVE-2026-42499
BDU:2026-07955

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Go: от 1.26.0 до 1.26.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://go.dev/cl/771520
- https://go.dev/issue/78987
- https://groups.google.com/g/golang-announce/c/qcCIEXso47M
- https://pkg.go.dev/vuln/GO-2026-4977
- https://bdu.fstec.ru/vul/2026-07955

Краткое описание: Выполнение произвольного кода в QCA7005

Идентификатор уязвимости: CVE-2026-25293
BDU:2026-07897

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: QCA7005: -

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

61 **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:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://docs.qualcomm.com/securitybulletin/may-2026-bulletin.html
- https://bdu.fstec.ru/vul/2026-07897

62

Краткое описание: Выполнение произвольного кода в Catalyst SD-WAN Manager

Идентификатор уязвимости: CVE-2026-20245
BDU:2026-07857

Идентификатор программной ошибки: CWE-116 Некорректная кодировка или очистка выходных данных

Уязвимый продукт: Catalyst SD-WAN Manager: -

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.

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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx
- https://bdu.fstec.ru/vul/2026-07857

63

Краткое описание: Выполнение произвольного кода в DWR-M920

Идентификатор уязвимости: CVE-2026-10878
BDU:2026-07858

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

Уязвимый продукт: DWR-M920: 1.1.7

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: 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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://github.com/7u7777/Dlink/blob/DWR-M920/formSmsManage.md
- https://bdu.fstec.ru/vul/2026-07858

64

Краткое описание: Выполнение произвольного кода в MLflow

Идентификатор уязвимости: CVE-2026-2651
BDU:2026-07859

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: MLflow: до 3.10.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

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:L/PR:L/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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://github.com/mlflow/mlflow/commit/d7290811d8f3c95366d80109424edc1fb1ad966f
- https://huntr.com/bounties/65beb119-d3e0-4e03-af2f-fa98f78f83dc
- https://bdu.fstec.ru/vul/2026-07859

65

Краткое описание: Отказ в обслуживании в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28318
BDU:2026-07860

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

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного POST-запроса.

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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28318
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-28318
- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_15-5-4-hotfix-1_release_notes.htm
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-07860

66

Краткое описание: Выполнение произвольного кода в radare2-mcp

Идентификатор уязвимости: CVE-2026-6942
BDU:2026-07861

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

Уязвимый продукт: radare2-mcp: до 1.6.0 включительно

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: 9.8 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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://github.com/radareorg/radare2-mcp/commit/482cde6500009112a8bc0b3fa8d2ef6180581ec0
- https://github.com/radareorg/radare2-mcp/issues/45
- https://www.vulncheck.com/advisories/radare2-mcp-os-command-injection-via-shell-metacharacter-bypass
- https://bdu.fstec.ru/vul/2026-07861

Краткое описание: Выполнение произвольного кода в Sogo

Идентификатор уязвимости: CVE-2026-39179
BDU:2026-07862

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

Уязвимый продукт: Sogo: до 5.12.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

67 **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: 10.0 AV:N/AC:L/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: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://www.sogo.nu/news/2026/sogo-v5127-released.html
- https://github.com/Alinto/sogo/releases
- https://bdu.fstec.ru/vul/2026-07862

Краткое описание: Выполнение произвольного кода в Sogo

Идентификатор уязвимости: CVE-2026-39178
BDU:2026-07863

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

Уязвимый продукт: Sogo: до 5.12.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

68 **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: 10.0 AV:N/AC:L/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: 2026-06-04 / 2026-06-04

Ссылки на источник:

- https://www.sogo.nu/news/2026/sogo-v5127-released.html
- https://github.com/Alinto/sogo/releases
- https://bdu.fstec.ru/vul/2026-07863

Краткое описание: Повышение привилегий в Moby Project

Идентификатор уязвимости: CVE-2026-34040
BDU:2026-07865

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

Уязвимый продукт: РЕД ОС: 8.0
Moby: до 29.3.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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.

69

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: 2026-05-02 / 2026-05-02

Ссылки на источник:

- https://github.com/moby/moby/releases/tag/docker-v29.3.1
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-34040
- https://bdu.fstec.ru/vul/2026-07865

Краткое описание: Выполнение произвольного кода в zlib

Идентификатор уязвимости: CVE-2026-3381
BDU:2026-07867

Идентификатор программной ошибки: CWE-1011 Авторизация

Уязвимый продукт: zlib: до 1.3.2
РЕД ОС: 8.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

70

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-jvq4-fjjq-g6w7
- https://github.com/madler/zlib/releases/tag/v1.3.2
- https://www.zlib.net
- https://github.com/pmqs/Compress-Raw-Zlib/issues/41
- https://github.com/madler/zlib
- https://7asecurity.com/blog/2026/02/zlib-7asecurity-audit
- https://www.cve.org/CVERecord?id=CVE-2026-27171
- https://7asecurity.com/blog/2026/02/zlib-7asecurity-audit/
- https://metacpan.org/release/PMQS/Compress-Raw-Zlib-2.221/source/Changes
- https://www.zlib.net/

- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-3381
- https://bdu.fstec.ru/vul/2026-07867

71

Краткое описание: Потеря целостности в LibreChat

Идентификатор уязвимости: CVE-2025-8850
BDU:2026-07878

Идентификатор программной ошибки: CWE-440 Отклонения от ожидаемого поведения

Уязвимый продукт: LibreChat: до 0.8.0-rc1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Потеря целостности

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: 2026-03-16 / 2026-03-16

Ссылки на источник:

- https://github.com/danny-avila/librechat/commit/7e4c8a5d0d2dbe5bf8fd272ff6acafb27d24744f
- https://huntr.com/bounties/8e615709-f4de-41e2-b194-f0d91ed7c75e
- https://bdu.fstec.ru/vul/2026-07878

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23406
BDU:2026-07883

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 4.17 до 6.6.130
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13

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

72 **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: 2026-04-07 / 2026-04-07

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026040112-CVE-2026-23406-0cb2@gregkh/
- https://git.kernel.org/stable/c/0510d1ba0976f97f521feb2b75b0572ea5df3ceb
- https://git.kernel.org/stable/c/383b7270faf42564f133134c2fc3c24bbae52615
- https://git.kernel.org/stable/c/5a184f7cbdeaad17e16dedf3c17d0cd622edfed8
- https://git.kernel.org/stable/c/8756b68edae37ff546c02091989a4ceab3f20abd
- https://git.kernel.org/stable/c/b73c1dff8a9d7eeaebabf8097a5b2de192f40913
- https://security-tracker.debian.org/tracker/CVE-2026-23406
- https://ubuntu.com/security/CVE-2026-23406
- https://bdu.fstec.ru/vul/2026-07883

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23408
BDU:2026-07885

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Linux: от 5.5 до 6.6.130
Ubuntu: 25.10
Debian GNU/Linux: 13

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

73 **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: 2026-04-07 / 2026-04-07

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026040113-CVE-2026-23408-1932@gregkh/
- https://git.kernel.org/stable/c/18b5233e860c294a847ee07869d93c0b8673a54b
- https://git.kernel.org/stable/c/55ef2af7490aaf72f8ffe11ec44c6bcb7eb2162a
- https://git.kernel.org/stable/c/5df0c44e8f5f619d3beb871207aded7c78414502
- https://git.kernel.org/stable/c/7998ab3010d2317643f91828f1853d954ef31387
- https://git.kernel.org/stable/c/86feeccd6b93ed94bd6655f30de80f163f8d5a45
- https://security-tracker.debian.org/tracker/CVE-2026-23408
- https://ubuntu.com/security/CVE-2026-23408
- https://bdu.fstec.ru/vul/2026-07885

74

Краткое описание: Повышение привилегий в MOVEit Automation

Идентификатор уязвимости: CVE-2026-4670
BDU:2026-07888

Идентификатор программной ошибки: CWE-305 Обход аутентификации с помощью стороннего недостатка

Уязвимый продукт: MOVEit Automation: до 2024.1.8

Категория уязвимого продукта: Серверное программное обеспечение и его 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.

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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://community.progress.com/s/article/MOVEit-Automation-Critical-Security-Alert-Bulletin-April-2026-CVE-2026-4670-CVE-2026-5174
- https://bdu.fstec.ru/vul/2026-07888

Краткое описание: Получение конфиденциальной информации в IntelliJ IDEA

Идентификатор уязвимости: CVE-2026-41882
BDU:2026-07890

Идентификатор программной ошибки: CWE-59 Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке")

Уязвимый продукт: IntelliJ IDEA: до 2026.1.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

75 **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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://www.jetbrains.com/privacy-security/issues-fixed/
- https://bdu.fstec.ru/vul/2026-07890

Краткое описание: Выполнение произвольного кода в QSC

Идентификатор уязвимости: CVE-2026-25254
BDU:2026-07894

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: QSC: 1.21.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

76 **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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://docs.qualcomm.com/securitybulletin/may-2026-bulletin.html
- https://bdu.fstec.ru/vul/2026-07894

77

Краткое описание: Повышение привилегий в QSC

Идентификатор уязвимости: CVE-2026-25255
BDU:2026-07895

Идентификатор программной ошибки: CWE-749 Доступны опасные методы или функции

Уязвимый продукт: QSC: 1.21.0
QPM: 3.0.127.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Злоупотребление функционалом.

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: 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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://docs.qualcomm.com/securitybulletin/may-2026-bulletin.html
- https://bdu.fstec.ru/vul/2026-07895

78

Краткое описание: Получение конфиденциальной информации в Next.js

Идентификатор уязвимости: CVE-2026-45109
BDU:2026-07875

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

Уязвимый продукт: Next.js: от 16.0.0 до 16.2.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2026-05-15 / 2026-05-15

Ссылки на источник:

- https://github.com/vercel/next.js/security/advisories/GHSA-26hh-7cqf-hhc6
- https://bdu.fstec.ru/vul/2026-07875