НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-01-26.1 | 26 января 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-23533	FreeRDP	Сетевой	ACE	2026-01-22	✓
2	Высокая	CVE-2026-23531	FreeRDP	Сетевой	ACE	2026-01-22	✓
3	Высокая	CVE-2026-23532	FreeRDP	Сетевой	ACE	2026-01-22	✓
4	Высокая	CVE-2026-23530	FreeRDP	Сетевой	ACE	2026-01-22	✓
5	Высокая	CVE-2026-23883	FreeRDP	Сетевой	ACE	2026-01-22	✓
6	Высокая	CVE-2026-23884	FreeRDP	Сетевой	ACE	2026-01-22	✓
7	Высокая	CVE-2026-23534	FreeRDP	Сетевой	ACE	2026-01-22	✓
8	Высокая	CVE-2026-24016	Fsas Technologies ServerView Agents for Windows	Локальный	ACE	2026-01-21	✓
9	Высокая	CVE-2025-13928	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	DoS	2026-01-21	✓
10	Высокая	CVE-2025-13927	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	DoS	2026-01-21	✓
11	Высокая	CVE-2026-23876	ImageMagick	Сетевой	ACE	2026-01-20	✓
12	Высокая	CVE-2025-47273	Junos Space	Сетевой	ACE	2026-01-19	✓

13	Высокая	CVE-2022-45061	Junos Space Security Director Policy Enforcer module	Сетевой	DoS	2026-01-19	✓
14	Высокая	CVE-2021-3737	Junos Space Security Director Policy Enforcer module	Сетевой	DoS	2026-01-19	✓
15	Критическая	CVE-2021-3177	Junos Space Security Director Policy Enforcer module	Сетевой	ACE	2026-01-19	✓
16	Высокая	CVE-2019-20907	Junos Space Security Director Policy Enforcer module	Сетевой	DoS	2026-01-19	✓
17	Высокая	CVE-2025-14409	Soda PDF Desktop	Локальный	ACE	2026-01-19	✗
18	Высокая	CVE-2025-14412	Soda PDF Desktop	Локальный	ACE	2026-01-19	✗
19	Высокая	CVE-2025-14413	Soda PDF Desktop	Локальный	WLF	2026-01-19	✗
20	Высокая	CVE-2025-14414	Soda PDF Desktop	Локальный	ACE	2026-01-19	✗
21	Высокая	CVE-2025-14406	Soda PDF Desktop	Локальный	ACE	2026-01-19	✗
22	Высокая	CVE-2025-38618	Google ChromeOS LTS	Локальный	PE	2026-01-19	✓
23	Высокая	CVE-2025-38350	Google ChromeOS LTS	Локальный	PE	2026-01-19	✓
24	Высокая	CVE-2025-38000	Google ChromeOS LTS	Локальный	PE	2026-01-19	✓
25	Высокая	CVE-2025-37890	Google ChromeOS LTS	Локальный	PE	2026-01-19	✓
26	Высокая	CVE-2025-37797	Google ChromeOS LTS	Локальный	DoS	2026-01-19	✓

27	Высокая	CVE-2026-0628	Google ChromeOS LTS	Сетевой	SB	2026-01-19	✓
28	Критическая	BDU:2025-10116	TrueConf Server	Сетевой	ACE	2025-08-20	✓
29	Высокая	BDU:2025-10114	TrueConf Server	Сетевой	OSI	2025-08-20	✓

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-23533
BDU:2026-00658

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: FreeRDP:
3.20.0 - 3.20.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

1 **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: 8.9 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-22 / 2026-01-22

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-32q9-m5qr-9j2v

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-23531
BDU:2026-00656

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: FreeRDP:
3.20.0 - 3.20.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

2 **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: 8.9 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-22 / 2026-01-22

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xj5h-9cr5-23c5

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-23532
BDU:2026-00657

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: FreeRDP:
3.20.0 - 3.20.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

3 **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: 8.9 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-22 / 2026-01-22

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-fq8c-87hj-7gvr

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-23530
BDU:2026-00655

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: FreeRDP:
3.20.0 - 3.20.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

4 **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: 8.9 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-22 / 2026-01-22

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-r4hv-852m-fq7p

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-23883
BDU:2026-00661

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: FreeRDP:
3.20.0 - 3.20.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

5 **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: 8.9 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-22 / 2026-01-22

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qcrr-85qx-4p6x

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-23884
BDU:2026-00662

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: FreeRDP:
3.20.0 - 3.20.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

6 **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: 8.9 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-22 / 2026-01-22

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-cfgj-vc84-f3pp

7

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-23534

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: FreeRDP:
3.20.0 - 3.20.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 8.9 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-22 / 2026-01-22

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-3frr-mp8w-4599

8

Краткое описание: Выполнение произвольного кода в Fsas Technologies ServerView Agents for Windows

Идентификатор уязвимости: CVE-2026-24016

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: ServerView Agents for Windows:
11.50.06 and previous versions

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-21 / 2026-01-21

Ссылки на источник:

- https://jvn.jp/en/jp/JVN65211823/index.html
- https://www.fsastech.com/ja-jp/resources/security/2026/0121.html

9

Краткое описание: Отказ в обслуживании в GitLab Community Edition (CE) and Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2025-13928

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: GitLab Enterprise Edition:
17.7.0 - 18.8.1
Gitlab Community Edition:
17.7.0 - 18.8.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса 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: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-21 / 2026-01-21

Ссылки на источник:

- https://about.gitlab.com/releases/2026/01/21/patch-release-gitlab-18-8-2-released/

10

Краткое описание: Отказ в обслуживании в GitLab Community Edition (CE) and Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2025-13927

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: GitLab Enterprise Edition:
11.9.0 - 18.8.1
Gitlab Community Edition:
11.9.0 - 18.8.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-21 / 2026-01-21

Ссылки на источник:

- https://about.gitlab.com/releases/2026/01/21/patch-release-gitlab-18-8-2-released/

11

Краткое описание: Выполнение произвольного кода в ImageMagick

Идентификатор уязвимости: CVE-2026-23876

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: ImageMagick:
6.9.13-0 - 7.1.2-12

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.2 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-20 / 2026-01-20

Ссылки на источник:

- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-r49w-jqq3-3gx8

12

Краткое описание: Выполнение произвольного кода в Junos Space

Идентификатор уязвимости: CVE-2025-47273

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

Уязвимый продукт: Juniper Junos Space:
до 24.1R5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-24-1R5-release

Краткое описание: Отказ в обслуживании в Junos Space Security Director Policy Enforcer module

Идентификатор уязвимости: CVE-2022-45061

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

Уязвимый продукт: Junos Space Security Director:
до 24.1R3

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

13 **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: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Policy-Enforcer-Multiple-vulnerabilities-in-Python-resolved-in-24-1R3-release

Краткое описание: Отказ в обслуживании в Junos Space Security Director Policy Enforcer module

Идентификатор уязвимости: CVE-2021-3737

Идентификатор программной ошибки: CWE-835 Бесконечный цикл (зацикливание)

Уязвимый продукт: Junos Space Security Director:
до 24.1R3

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированного 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.

14

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

Оценка CVSSv4: 1.2 AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Policy-Enforcer-Multiple-vulnerabilities-in-Python-resolved-in-24-1R3-release

Краткое описание: Выполнение произвольного кода в Junos Space Security Director Policy Enforcer module

Идентификатор уязвимости: CVE-2021-3177

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

Уязвимый продукт: Junos Space Security Director:
до 24.1R3

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

15

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Policy-Enforcer-Multiple-vulnerabilities-in-Python-resolved-in-24-1R3-release

16

Краткое описание: Отказ в обслуживании в Junos Space Security Director Policy Enforcer module

Идентификатор уязвимости: CVE-2019-20907

Идентификатор программной ошибки: CWE-835 Бесконечный цикл (зацикливание)

Уязвимый продукт: Junos Space Security Director:
до 24.1R3

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Policy-Enforcer-Multiple-vulnerabilities-in-Python-resolved-in-24-1R3-release

Краткое описание: Выполнение произвольного кода в Soda PDF Desktop

Идентификатор уязвимости: CVE-2025-14409

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Soda PDF Desktop:
все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1082/

Краткое описание: Выполнение произвольного кода в Soda PDF Desktop

Идентификатор уязвимости: CVE-2025-14412

Идентификатор программной ошибки: CWE-357 Недостаточно очевидное предупреждение об опасных операциях

Уязвимый продукт: Soda PDF Desktop:
все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1085/

Краткое описание: Запись локальных файлов в Soda PDF Desktop

Идентификатор уязвимости: CVE-2025-14413

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

Уязвимый продукт: Soda PDF Desktop:
все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Запись локальных файлов

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1086/

Краткое описание: Выполнение произвольного кода в Soda PDF Desktop

Идентификатор уязвимости: CVE-2025-14414

Идентификатор программной ошибки: CWE-357 Недостаточно очевидное предупреждение об опасных операциях

Уязвимый продукт: Soda PDF Desktop:
все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1087/

Краткое описание: Выполнение произвольного кода в Soda PDF Desktop

Идентификатор уязвимости: CVE-2025-14406

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

Уязвимый продукт: Soda PDF Desktop:
все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 5.9 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1079/

22

Краткое описание: Повышение привилегий в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-38618

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS:
до 138.0.7204.301

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: 5.9 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/01/long-term-support-channel-update-for_16.html

23

Краткое описание: Повышение привилегий в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-38350

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS:
до 138.0.7204.301

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: 5.9 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/01/long-term-support-channel-update-for_16.html

Краткое описание: Повышение привилегий в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-38000

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS:
до 138.0.7204.301

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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

Оценка CVSSv4: 5.9 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/01/long-term-support-channel-update-for_16.html

Краткое описание: Повышение привилегий в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-37890

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS:
до 138.0.7204.301

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv4: 5.9 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/01/long-term-support-channel-update-for_16.html

26

Краткое описание: Отказ в обслуживании в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-37797

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Chrome OS:
до 138.0.7204.301

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных 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: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: 4.3 AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/01/long-term-support-channel-update-for_16.html

27

Краткое описание: Обход безопасности в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-0628

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: Chrome OS:
до 138.0.7204.301

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-19 / 2026-01-19

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/01/long-term-support-channel-update-for_16.html

Краткое описание: Выполнение произвольного кода в TrueConf Server

Идентификатор уязвимости: BDU:2025-10116

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

Уязвимый продукт: TrueConf Server:
до 5.3.7
до 5.4.6
до 5.5.1
до 5.5.1.10180

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

28

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: 0.0 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: 2025-08-20 / 2025-12-11

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-10116
- https://trueconf.ru/blog/update/trueconf-server-security-update-08-25

29

Краткое описание: Получение конфиденциальной информации в TrueConf Server

Идентификатор уязвимости: BDU:2025-10114

Идентификатор программной ошибки: CWE-228 Некорректная обработка синтаксически неверных структур

Уязвимый продукт: TrueConf Server:
до 5.3.7
до 5.5.1
до 5.4.6
до 5.5.1.10180

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса 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: 0.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-20 / 2025-12-11

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-10114
- https://trueconf.ru/blog/update/trueconf-server-security-update-08-25