НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-02-21.1 | 21 февраля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Средняя	CVE-2023-5253	Siemens RUGGEDCOM APE1808 devices with Nozomi Guardian/CMC	Сетевой	SB	2024-02-20	✗
2	Высокая	CVE-2024-24794	Imaging Data Commons libdicom	Сетевой	ACE	2024-02-20	✓
3	Высокая	CVE-2024-24793	Imaging Data Commons libdicom	Сетевой	ACE	2024-02-20	✓
4	Высокая	CVE-2024-1553	Mozilla Thunderbird	Сетевой	ACE	2024-02-21	✓
5	Высокая	CVE-2024-1546	Mozilla Thunderbird	Сетевой	ACE	2024-02-21	✓
6	Высокая	CVE-2024-1674	Google Chrome	Сетевой	OSI	2024-02-21	✓
7	Высокая	CVE-2024-1672	Google Chrome	Сетевой	OSI	2024-02-21	✓
8	Высокая	CVE-2024-1671	Google Chrome	Сетевой	OSI	2024-02-21	✓
9	Высокая	CVE-2024-1670	Google Chrome	Сетевой	ACE	2024-02-21	✓
10	Высокая	CVE-2024-1669	Google Chrome	Сетевой	ACE	2024-02-21	✓
11	Высокая	CVE-2024-22250	VMware Enhanced Authentication Plug-in (EAP)	Локальный	OSI	2024-02-20	✗
12	Критическая	CVE-2024-22245	VMware Enhanced Authentication Plug-in (EAP)	Сетевой	OSI	2024-02-20	✗
13	Критическая	CVE-2023-49109	Apache DolphinScheduler	Сетевой	ACE	2024-02-20	✓

14	Высокая	CVE-2024-1557	Mozilla Firefox	Сетевой	ACE	2024-02-20	✓
15	Высокая	CVE-2024-1553	Mozilla Firefox	Сетевой	ACE	2024-02-20	✓
16	Высокая	CVE-2024-1546	Mozilla Firefox	Сетевой	ACE	2024-02-20	✓
17	Высокая	CVE-2023-50291	Apache Solr	Сетевой	OSI	2024-02-20	✓
18	Высокая	CVE-2023-50292	Apache Solr	Сетевой	ACE	2024-02-20	✓
19	Критическая	CVE-2024-22369	Apache Camel	Сетевой	ACE	2024-02-20	✓
20	Критическая	CVE-2024-23114	Apache Camel	Сетевой	ACE	2024-02-20	✓
21	Критическая	CVE-2024-23807	Apache Xerces C++	Сетевой	ACE	2024-02-20	✓
22	Высокая	CVE-2023-6764	Zyxel firewalls and APs	Сетевой	ACE	2024-02-20	✓
23	Высокая	CVE-2023-6932	Google ChromeOS TLS	Локальный	ACE	2024-02-19	✓
24	Высокая	CVE-2023-6817	Google ChromeOS TLS	Локальный	PE	2024-02-19	✓
25	Высокая	CVE-2023-6931	Google ChromeOS TLS	Локальный	PE	2024-02-19	✓
26	Высокая	CVE-2023-51042	Google ChromeOS TLS	Локальный	PE	2024-02-19	✓
27	Критическая	CVE-2024-0808	Google ChromeOS TLS	Сетевой	ACE	2024-02-19	✓
28	Высокая	CVE-2024-0807	Google ChromeOS TLS	Сетевой	ACE	2024-02-19	✓

29	Критическая	CVE-2023-6345	Google ChromeOS TLS	Сетевой	ACE	2024-02-19	✓
30	Высокая	CVE-2023-51440	Siemens CP343-1 Devices	Сетевой	DoS	2024-02-15	✗
31	Критическая	CVE-2024-23113	FortiOS	Сетевой	ACE	2024-02-09	✓
32	Критическая	CVE-2024-21762	FortiOS SSL-VPN	Сетевой	ACE	2024-02-09	✓
33	Высокая	CVE-2023-45581	FortiClientEMS	Сетевой	PE	2024-02-09	✓
34	Критическая	CVE-2024-23108	FortiSIEM	Сетевой	ACE	2023-10-12	✓
35	Критическая	CVE-2024-23109	FortiSIEM	Сетевой	ACE	2023-10-12	✓
36	Критическая	CVE-2023-34992	FortiSIEM	Сетевой	ACE	2023-10-12	✓
37	Высокая	CVE-2024-23812	SINEC NMS	Смежная сеть	ACE	2024-02-13	✓
38	Высокая	CVE-2024-23811	SINEC NMS	Смежная сеть	ACE	2024-02-13	✓
39	Высокая	CVE-2024-23810	SINEC NMS	Смежная сеть	ACE	2024-02-13	✓

1

Краткое описание: Обход безопасности в Siemens RUGGEDCOM APE1808 devices with Nozomi Guardian/CMC

Идентификатор уязвимости: CVE-2023-5253

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

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: обход безопасности

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

Оценка CVSSv3: 5.3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-665034.txt
- https://bdu.fstec.ru/vul/2024-00887

2

Краткое описание: Выполнение произвольного кода в Imaging Data Commons libdicom

Идентификатор уязвимости: CVE-2024-24794

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: libdicom: 1.0.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://www.talosintelligence.com/vulnerability_reports/TALOS-2024-1931

Краткое описание: Выполнение произвольного кода в Imaging Data Commons libdicom

Идентификатор уязвимости: CVE-2024-24793

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: libdicom: 1.0.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://www.talosintelligence.com/vulnerability_reports/TALOS-2024-1931

4

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-1553

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

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 115.7.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-21 / 2024-02-21

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-07/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-1546

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 115.7.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-21 / 2024-02-21

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-07/

6

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-1674

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 121.0.6167.185

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-21 / 2024-02-21

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html
- http://crbug.com/40095183

7

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-1672

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 121.0.6167.185

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-21 / 2024-02-21

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html
- http://crbug.com/41485789

8

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-1671

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 121.0.6167.185

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-21 / 2024-02-21

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html
- http://crbug.com/41487933

9

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-1670

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 121.0.6167.185

Категория уязвимого продукта: Прикладное программное обеспечение

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

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:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-21 / 2024-02-21

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html
- http://crbug.com/41481374

10

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-1669

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 121.0.6167.185

Категория уязвимого продукта: Прикладное программное обеспечение

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

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:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-21 / 2024-02-21

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html
- http://crbug.com/41495060

Краткое описание: Получение конфиденциальной информации в VMware Enhanced Authentication Plug-in (EAP)

Идентификатор уязвимости: CVE-2024-22250

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

Уязвимый продукт: Enhanced Authentication Plug-in (EAP): все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2024-0003.html

Краткое описание: Получение конфиденциальной информации в VMware Enhanced Authentication Plug-in (EAP)

Идентификатор уязвимости: CVE-2024-22245

Идентификатор программной ошибки: CWE-294 Обход аутентификации при помощи перехвата и воспроизведения

Уязвимый продукт: Enhanced Authentication Plug-in (EAP): все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2024-0003.html

13

Краткое описание: Выполнение произвольного кода в Apache DolphinScheduler

Идентификатор уязвимости: CVE-2023-49109

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: DolphinScheduler: 3.0.0 - 3.2.0

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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://github.com/apache/dolphinscheduler/pull/14991
- http://www.openwall.com/lists/oss-security/2024/02/20/4
- http://lists.apache.org/thread/llnghrd72gbfhwh4tn68zvl1hzl9gxn6

14

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-1557

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

Уязвимый продукт: Mozilla Firefox: 120.0 - 122.0.1
Firefox for Android: 120.0 - 122.1.0
Firefox for iOS: 120.0 - 122.2

Категория уязвимого продукта: Прикладное программное обеспечение

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:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-05/

15

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-1553

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 122.0.1
Firefox ESR: 102.0 - 115.7.0
Firefox for Android: 100.1.0 - 122.1.0
Firefox for iOS: 100.1 - 122.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

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:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-05/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-06/

16

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-1546

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Mozilla Firefox: 100.0 - 122.0.1
Firefox ESR: 102.0 - 115.7.0
Firefox for Android: 100.1.0 - 122.1.0
Firefox for iOS: 100.1 - 122.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

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:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-05/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-06/

17

Краткое описание: Получение конфиденциальной информации в Apache Solr

Идентификатор уязвимости: CVE-2023-50291

Идентификатор программной ошибки: CWE-522 Недостаточно надежная защита учетных данных

Уязвимый продукт: Apache Solr: 6.0 - 9.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://solr.apache.org/security.html#cve-2023-50291-apache-solr-can-leak-certain-passwords-due-to-system-property-redaction-logic-inconsistencies
- http://www.openwall.com/lists/oss-security/2024/02/09/4
- http://lists.apache.org/thread/w76gwqhl523pv7o9bkcf9g7znffq8m6q
- https://bdu.fstec.ru/vul/2024-01302

18

Краткое описание: Выполнение произвольного кода в Apache Solr

Идентификатор уязвимости: CVE-2023-50292

Идентификатор программной ошибки: CWE-732 Некорректные разрешения для критически важных ресурсов

Уязвимый продукт: Apache Solr: 8.10.0 - 9.2.1

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:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://solr.apache.org/security.html#cve-2023-50298-apache-solr-can-expose-zookeeper-credentials-via-streaming-expressions
- http://www.openwall.com/lists/oss-security/2024/02/09/3
- http://lists.apache.org/thread/jkfgxrjmpo9tqv8yqbnnbfbsorpncch4

Краткое описание: Выполнение произвольного кода в Apache Camel

Идентификатор уязвимости: CVE-2024-22369

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Apache Camel: 3.0.0 - 4.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

19 **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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://lists.apache.org/thread/jljx6bjno5nc5m7l0tby3zf4s7g1j0hg

Краткое описание: Выполнение произвольного кода в Apache Camel

Идентификатор уязвимости: CVE-2024-23114

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Apache Camel: 3.0.0 - 4.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://lists.apache.org/thread/hj9y0l6q3vqsphp1nfw7tpk0b20979bj

21

Краткое описание: Выполнение произвольного кода в Apache Xerces C++

Идентификатор уязвимости: CVE-2024-23807

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Apache Xerces C++: 3.0.0 - 3.2.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://lists.apache.org/thread/c497tgn864tsbm8w0bo3f0d81s07zk9r
- http://issues.apache.org/jira/browse/XERCESC-2188

22

Краткое описание: Выполнение произвольного кода в Zyxel firewalls and APs

Идентификатор уязвимости: CVE-2023-6764

Идентификатор программной ошибки: CWE-134 Использование форматной строки, контролируемой извне

Уязвимый продукт: ATP series: 4.32 - 5.37 Patch 1
USG FLEX series: 4.50 - 5.37 Patch 1
USG FLEX 50W: 4.16 - 5.37 Patch 1
USG20W-VPN: 4.16 - 5.37 Patch 1

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.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-20 / 2024-02-20

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-aps-02-20-2024

23

Краткое описание: Выполнение произвольного кода в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2023-6932

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 114.0.5735.351

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-19 / 2024-02-19

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_16.html
- https://bdu.fstec.ru/vul/2023-09022

24

Краткое описание: Повышение привилегий в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2023-6817

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 114.0.5735.351

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

Способ эксплуатации: Не определено

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-19 / 2024-02-19

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_16.html
- https://bdu.fstec.ru/vul/2023-08958

25

Краткое описание: Повышение привилегий в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2023-6931

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Chrome OS: до 114.0.5735.351

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

Способ эксплуатации: Не определено

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-19 / 2024-02-19

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_16.html
- https://bdu.fstec.ru/vul/2023-09023

26

Краткое описание: Повышение привилегий в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2023-51042

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 114.0.5735.351

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

Способ эксплуатации: Не определено

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-19 / 2024-02-19

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_16.html
- https://bdu.fstec.ru/vul/2024-00866

27

Краткое описание: Выполнение произвольного кода в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2024-0808

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: Chrome OS: до 114.0.5735.351

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-19 / 2024-02-19

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_16.html
- https://bdu.fstec.ru/vul/2024-00841

28

Краткое описание: Выполнение произвольного кода в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2024-0807

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 114.0.5735.351

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

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

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-19 / 2024-02-19

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_16.html
- https://bdu.fstec.ru/vul/2024-00845

29

Краткое описание: Выполнение произвольного кода в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2023-6345

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Chrome OS: до 114.0.5735.351

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

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

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-19 / 2024-02-19

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_16.html
- https://bdu.fstec.ru/vul/2023-08264

Краткое описание: Отказ в обслуживании в Siemens CP343-1 Devices

Идентификатор уязвимости: CVE-2023-51440

Идентификатор программной ошибки: CWE-940 Некорректная проверка источника для канала связи

Уязвимый продукт: SIMATIC CP 343-1: все версии
SIMATIC CP 343-1 LEAN: все версии
SIPLUS NET CP 343-1: все версии
SIPLUS NET CP 343-1 Lean: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

30

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-15 / 2024-02-15

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-516818.html

31

Краткое описание: Выполнение произвольного кода в FortiOS

Идентификатор уязвимости: CVE-2024-23113

Идентификатор программной ошибки: CWE-134 Использование форматной строки, контролируемой извне

Уязвимый продукт: FortiOS: с версии 7.0.0 по 7.4.2

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

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-09 / 2024-02-09

Ссылки на источник:

- http://www.fortiguard.com/psirt/FG-IR-24-029
- https://bdu.fstec.ru/vul/2024-01122

32

Краткое описание: Выполнение произвольного кода в FortiOS SSL-VPN

Идентификатор уязвимости: CVE-2024-21762

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FortiOS: с версии 6.0.0 по 7.4.2

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

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-09 / 2024-02-09

Ссылки на источник:

- http://www.fortiguard.com/psirt/FG-IR-24-015
- https://bdu.fstec.ru/vul/2024-01125

Краткое описание: Повышение привилегий в FortiClientEMS

Идентификатор уязвимости: CVE-2023-45581

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: FortiClientEMS: с версии 6.2.0 по 7.2.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: повышение привилегий

33 **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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-09 / 2024-02-09

Ссылки на источник:

- http://www.fortiguard.com/psirt/FG-IR-23-357

Краткое описание: Выполнение произвольного кода в FortiSIEM

Идентификатор уязвимости: CVE-2024-23108

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

Уязвимый продукт: FortiSIEM: с версии 6.4.0 по 7.1.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-12 / 2023-10-12

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-130
- https://bdu.fstec.ru/vul/2024-01082

Краткое описание: Выполнение произвольного кода в FortiSIEM

Идентификатор уязвимости: CVE-2024-23109

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

Уязвимый продукт: FortiSIEM: с версии 6.4.0 по 7.1.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: выполнение произвольного кода

35

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-12 / 2023-10-12

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-130
- https://bdu.fstec.ru/vul/2024-01127

Краткое описание: Выполнение произвольного кода в FortiSIEM

Идентификатор уязвимости: CVE-2023-34992

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

Уязвимый продукт: FortiSIEM: с версии 6.4.0 по 7.1.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-12 / 2023-10-12

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-130
- https://bdu.fstec.ru/vul/2023-06702

Краткое описание: Выполнение произвольного кода в SINEC NMS

Идентификатор уязвимости: CVE-2024-23812

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

Уязвимый продукт: SINEC NMS: до версии V2.0 SP1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

37

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-13 / 2024-02-13

Ссылки на источник:

38

Краткое описание: Выполнение произвольного кода в SINEC NMS

Идентификатор уязвимости: CVE-2024-23811

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

Уязвимый продукт: SINEC NMS: до версии V2.0 SP1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-13 / 2024-02-13

Ссылки на источник:

Краткое описание: Выполнение произвольного кода в SINEC NMS

Идентификатор уязвимости: CVE-2024-23810

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

Уязвимый продукт: SINEC NMS: до версии V2.0 SP1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

39

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-13 / 2024-02-13

Ссылки на источник: