НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-07-08.1 | 8 июля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-36983	Splunk Enterprise	Сетевой	ACE	2024-07-01	✓
2	Высокая	CVE-2024-36984	Splunk Enterprise	Сетевой	ACE	2024-07-01	✓
3	Высокая	CVE-2024-36985	Splunk Enterprise	Сетевой	ACE	2024-07-01	✓
4	Высокая	CVE-2024-36982	Splunk Enterprise	Сетевой	DoS	2024-07-01	✓
5	Высокая	CVE-2024-36997	Splunk Enterprise	Сетевой	XSS\CSS	2024-07-01	✓
6	Высокая	CVE-2024-36991	Splunk Enterprise	Сетевой	RLF	2024-07-01	✓
7	Высокая	CVE-2023-52168	7-Zip	Сетевой	ACE	2024-07-03	✓
8	Высокая	CVE-2024-29506	Artifex Ghostscript	Сетевой	ACE	2024-07-05	✓
9	Высокая	CVE-2024-29507	Artifex Ghostscript	Сетевой	ACE	2024-07-05	✓
10	Высокая	CVE-2024-29508	Artifex Ghostscript	Сетевой	ACE	2024-07-05	✓
11	Высокая	CVE-2023-4807	ICONICS Products	Локальный	DoS	2024-07-03	✓
12	Высокая	CVE-2022-2650	ICONICS Products	Локальный	OSI	2024-07-03	✓
13	Высокая	CVE-2024-37147	GLPI	Сетевой	WLF	2024-07-04	✓

14	Критическая	CVE-2024-37149	GLPI	Сетевой	ACE	2024-07-04	✓
15	Критическая	CVE-2024-37148	GLPI	Сетевой	ACE	2024-07-04	✓
16	Высокая	CVE-2024-39350	Synology Camera BC500 and TC500	Смежная сеть	SB	2024-07-02	✓
17	Критическая	CVE-2024-39349	Synology Camera BC500 and TC500	Сетевой	ACE	2024-07-02	✓
18	Высокая	CVE-2024-39352	Synology Camera BC500 and TC500	Сетевой	PE	2024-07-02	✓
19	Критическая	CVE-2024-23692	Rejetto HTTP File Server (HFS)	Сетевой	ACE	2024-07-05	✗
20	Высокая	CVE-2024-22354	InfoSphere Master Data Management	Сетевой	OSI	2024-07-05	✓
21	Высокая	CVE-2024-32937	Grandstream GXP2135	Сетевой	ACE	2024-07-04	✓
22	Высокая	CVE-2022-2650	wger	Локальный	OSI	2024-07-03	✓
23	Критическая	CVE-2024-4708	mySCADA myPRO	Сетевой	ACE	2024-07-03	✓
24	Высокая	CVE-2024-38519	yt-dlp	Локальный	ACE	2024-07-02	✓
25	Критическая	CVE-2024-0769	D-Link DIR-859	Сетевой	RLF	2024-07-01	✗
26	Высокая	CVE-2024-20399	Cisco NX-OS Software	Локальный	ACE	2024-07-01	✗
27	Высокая	CVE-2024-36387	Apache HTTP Server	Сетевой	DoS	2024-07-01	✓
28	Высокая	CVE-2024-38475	Apache HTTP Server	Сетевой	ACE	2024-07-01	✓

29	Критическая	CVE-2024-38476	Apache HTTP Server	Сетевой	CSRF	2024-07-01	✓
30	Высокая	CVE-2024-38477	Apache HTTP Server	Сетевой	DoS	2024-07-01	✓
31	Критическая	CVE-2024-39309	parse-server	Сетевой	ACE	2024-07-01	✓
32	Критическая	CVE-2024-38441	Netatalk	Сетевой	ACE	2024-07-01	✓
33	Критическая	CVE-2024-38440	Netatalk	Сетевой	ACE	2024-07-01	✓
34	Критическая	CVE-2024-38439	Netatalk	Сетевой	ACE	2024-07-01	✓
35	Высокая	CVE-2024-6387	OpenSSH	Сетевой	ACE	2024-07-01	✓
36	Критическая	CVE-2024-2973	Juniper Session Smart Router	Сетевой	SB	2024-07-01	✓

1

Краткое описание: Выполнение произвольного кода в Splunk Enterprise

Идентификатор уязвимости: CVE-2024-36983

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

Уязвимый продукт: Splunk Enterprise: 9.0.0 - 9.2.1

Категория уязвимого продукта: Средства защиты информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://advisory.splunk.com/advisories/SVD-2024-0703
- http://research.splunk.com/application/1cf58ae1-9177-40b8-a26c-8966040f11ae/

2

Краткое описание: Выполнение произвольного кода в Splunk Enterprise

Идентификатор уязвимости: CVE-2024-36984

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Splunk Enterprise: 9.0.0 - 9.2.1

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: 8.8 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: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://advisory.splunk.com/advisories/SVD-2024-0704
- http://research.splunk.com/application/1cf58ae1-9177-40b8-a26c-8966040f11ae/

3

Краткое описание: Выполнение произвольного кода в Splunk Enterprise

Идентификатор уязвимости: CVE-2024-36985

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

Уязвимый продукт: Splunk Enterprise: 9.0.0 - 9.2.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных 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: 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: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://advisory.splunk.com/advisories/SVD-2024-0705
- http://research.splunk.com/application/8598f9de-bba8-42a4-8ef0-12e1adda4131

4

Краткое описание: Отказ в обслуживании в Splunk Enterprise

Идентификатор уязвимости: CVE-2024-36982

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Splunk Enterprise: 9.0.0 - 9.2.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://advisory.splunk.com/advisories/SVD-2024-0702

Краткое описание: Межсайтовый скриптинг в Splunk Enterprise

Идентификатор уязвимости: CVE-2024-36997

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

Уязвимый продукт: Splunk Enterprise: 9.0.0 - 9.2.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Внедрение HTML-кода.

Последствия эксплуатации: Межсайтовый скриптинг

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://advisory.splunk.com/advisories/SVD-2024-0717
- http://research.splunk.com/application/ed1209ef-228d-4dab-9856-be9369925a5c

6

Краткое описание: Чтение локальных файлов в Splunk Enterprise

Идентификатор уязвимости: CVE-2024-36991

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

Уязвимый продукт: Splunk Enterprise: 9.0.0 - 9.2.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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.

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: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://advisory.splunk.com/advisories/SVD-2024-0711
- http://research.splunk.com/application/e7c2b064-524e-4d65-8002-efce808567aa

7

Краткое описание: Выполнение произвольного кода в 7-Zip

Идентификатор уязвимости: CVE-2023-52168

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

Уязвимый продукт: 7-Zip: 2.00 - 24.00

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: 2024-07-03 / 2024-07-03

Ссылки на источник:

- http://seclists.org/oss-sec/2024/q3/24
- http://dfir.ru/2024/06/19/vulnerabilities-in-7-zip-and-ntfs3/
- https://bdu.fstec.ru/vul/2024-04975

8

Краткое описание: Выполнение произвольного кода в Artifex Ghostscript

Идентификатор уязвимости: CVE-2024-29506

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Ghostscript: 9.00 - 10.02.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2024-07-05 / 2024-07-05

Ссылки на источник:

- http://bugs.ghostscript.com/show_bug.cgi?id=707510
- http://git.ghostscript.com/?p=ghostpdl.git%3Bh=77dc7f699beba606937b7ea23b50cf5974fa64b1
- http://www.openwall.com/lists/oss-security/2024/07/03/7

9

Краткое описание: Выполнение произвольного кода в Artifex Ghostscript

Идентификатор уязвимости: CVE-2024-29507

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Ghostscript: 9.00 - 10.02.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2024-07-05 / 2024-07-05

Ссылки на источник:

- http://bugs.ghostscript.com/show_bug.cgi?id=707510
- http://git.ghostscript.com/?p=ghostpdl.git%3Ba=commitdiff%3Bh=7745dbe24514
- http://www.openwall.com/lists/oss-security/2024/07/03/7

10

Краткое описание: Выполнение произвольного кода в Artifex Ghostscript

Идентификатор уязвимости: CVE-2024-29508

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

Уязвимый продукт: Ghostscript: 9.00 - 10.02.1

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: 8.8 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: 2024-07-05 / 2024-07-05

Ссылки на источник:

- http://bugs.ghostscript.com/show_bug.cgi?id=707510
- http://git.ghostscript.com/?p=ghostpdl.git%3Bh=ff1013a0ab485b66783b70145e342a82c670906a
- http://www.openwall.com/lists/oss-security/2024/07/03/7

Краткое описание: Отказ в обслуживании в ICONICS Products

Идентификатор уязвимости: CVE-2023-4807

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ICONICS Suite: до 10.97.2
MobileHMI: до 10.97.2
Energy AnalytiX: до 10.97.2
Hyper Historian: до 10.97.2
GENESIS64: до 10.97.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

11 **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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-03 / 2024-07-03

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-184-03
- https://bdu.fstec.ru/vul/2023-05872

Краткое описание: Получение конфиденциальной информации в ICONICS Products

Идентификатор уязвимости: CVE-2022-2650

Идентификатор программной ошибки: CWE-307 Некорректное ограничение количества неудачных попыток аутентификации

Уязвимый продукт: ICONICS Suite: до 10.97.2
MobileHMI: до 10.97.2
Energy AnalytiX: до 10.97.2
Hyper Historian: до 10.97.2
GENESIS64: до 10.97.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

12

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-03 / 2024-07-03

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-184-03

13

Краткое описание: Запись локальных файлов в GLPI

Идентификатор уязвимости: CVE-2024-37147

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

Уязвимый продукт: GLPI: 10.0.0 - 10.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись 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.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/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: 2024-07-04 / 2024-07-04

Ссылки на источник:

- http://github.com/glpi-project/glpi/releases/tag/10.0.16

14

Краткое описание: Выполнение произвольного кода в GLPI

Идентификатор уязвимости: CVE-2024-37149

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

Уязвимый продукт: GLPI: 10.0.0 - 10.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-04 / 2024-07-04

Ссылки на источник:

- http://github.com/glpi-project/glpi/releases/tag/10.0.16

Краткое описание: Выполнение произвольного кода в GLPI

Идентификатор уязвимости: CVE-2024-37148

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

Уязвимый продукт: GLPI: 10.0.0 - 10.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

15

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: 2024-07-04 / 2024-07-04

Ссылки на источник:

- http://github.com/glpi-project/glpi/releases/tag/10.0.16

Краткое описание: Обход безопасности в Synology Camera BC500 and TC500

Идентификатор уязвимости: CVE-2024-39350

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: BC500: до 1.0.7-0298
TC500: до 1.0.7-0298

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

16

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-02 / 2024-07-02

Ссылки на источник:

- http://www.synology.com/en-global/security/advisory/Synology_SA_23_15

Краткое описание: Выполнение произвольного кода в Synology Camera BC500 and TC500

Идентификатор уязвимости: CVE-2024-39349

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

Уязвимый продукт: BC500: до 1.0.7-0298
TC500: до 1.0.7-0298

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

17

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: 2024-07-02 / 2024-07-02

Ссылки на источник:

- http://www.synology.com/en-global/security/advisory/Synology_SA_23_15

Краткое описание: Повышение привилегий в Synology Camera BC500 and TC500

Идентификатор уязвимости: CVE-2024-39352

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: TC500: до 1.0.7-0298
BC500: до 1.0.7-0298

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

18 **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:H/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-02 / 2024-07-02

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-834/
- http://www.synology.com/en-id/security/advisory/Synology_SA_23_15

19

Краткое описание: Выполнение произвольного кода в Rejetto HTTP File Server (HFS)

Идентификатор уязвимости: CVE-2024-23692

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

Уязвимый продукт: HFS: 2.2 - 2.3m

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2024-07-05 / 2024-07-05

Ссылки на источник:

- http://vulncheck.com/advisories/rejetto-unauth-rce
- http://mohemiv.com/all/rejetto-http-file-server-2-3m-unauthenticated-rce/
- http://github.com/rapid7/metasploit-framework/pull/19240
- http://asec.ahnlab.com/en/67650/

Краткое описание: Получение конфиденциальной информации в InfoSphere Master Data Management

Идентификатор уязвимости: CVE-2024-22354

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: InfoSphere Master Data Management: 11.6 - 12.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-05 / 2024-07-05

Ссылки на источник:

- http://www.ibm.com/support/pages/node/7156931

Краткое описание: Выполнение произвольного кода в Grandstream GXP2135

Идентификатор уязвимости: CVE-2024-32937

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

Уязвимый продукт: GXP2135: 1.0.9.129 - 1.0.11.79

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

21

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

Оценка CVSSv3: 8.1 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: 2024-07-04 / 2024-07-04

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2024-1978

Краткое описание: Получение конфиденциальной информации в wger

Идентификатор уязвимости: CVE-2022-2650

Идентификатор программной ошибки: CWE-307 Некорректное ограничение количества неудачных попыток аутентификации

Уязвимый продукт: wger: 1.0 - 2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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: 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: 2024-07-03 / 2024-07-03

Ссылки на источник:

- http://huntr.dev/bounties/f0d85efa-4e78-4b1d-848f-edea115af64b
- http://github.com/wger-project/wger/commit/5e3167e3a2dc95836fa2607fe201524c031a2c4c

23

Краткое описание: Выполнение произвольного кода в mySCADA myPRO

Идентификатор уязвимости: CVE-2024-4708

Идентификатор программной ошибки: CWE-259 Использование жестко закодированного пароля

Уязвимый продукт: myPRO: до 8.31.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Использование жестко закодированных учетных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-03 / 2024-07-03

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-184-02
- http://www.myscada.org/mypro/

Краткое описание: Выполнение произвольного кода в yt-dlp

Идентификатор уязвимости: CVE-2024-38519

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: yt-dlp: 2021.01.07 - 2024.05.27

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-02 / 2024-07-02

Ссылки на источник:

- http://github.com/yt-dlp/yt-dlp/releases/tag/2024.07.01
- http://github.com/yt-dlp/yt-dlp/security/advisories/GHSA-79w7-vh3h-8g4j

25

Краткое описание: Чтение локальных файлов в D-Link DIR-859

Идентификатор уязвимости: CVE-2024-0769

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

Уязвимый продукт: DIR-859: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Чтение локальных файлов

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://vuldb.com/?id.251666
- http://vuldb.com/?ctiid.251666
- http://github.com/c2dc/cve-reported/blob/main/CVE-2024-0769/CVE-2024-0769.md
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10371

Краткое описание: Выполнение произвольного кода в Cisco NX-OS Software

Идентификатор уязвимости: CVE-2024-20399

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

Уязвимый продукт: Cisco NX-OS: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

26

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwj97007
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwj97009
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwj97011
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwj94682
- https://bdu.fstec.ru/vul/2024-04937

Краткое описание: Отказ в обслуживании в Apache HTTP Server

Идентификатор уязвимости: CVE-2024-36387

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Apache HTTP Server: 2.4.55 - 2.4.59

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://lists.apache.org/thread/8dslvr98bxcvzxz7cwq6h3q6h2xgk0oo

28

Краткое описание: Выполнение произвольного кода в Apache HTTP Server

Идентификатор уязвимости: CVE-2024-38475

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Apache HTTP Server: 2.4 - 2.4.59

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.

Оценка CVSSv3: 8.1 AV:N/AC:H/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: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://lists.apache.org/thread/tzks8jdmh39hbl723d1xq61mcl4ndv13
- https://bdu.fstec.ru/vul/2024-04936

Краткое описание: Подделка запросов на стороне сервера в Apache HTTP Server

Идентификатор уязвимости: CVE-2024-38476

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

Уязвимый продукт: Apache HTTP Server: 2.4 - 2.4.59

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Подделка запросов на стороне сервера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://lists.apache.org/thread/p2xfjsvpogyrg4hw9cjs2nrnqnl34qf0

Краткое описание: Отказ в обслуживании в Apache HTTP Server

Идентификатор уязвимости: CVE-2024-38477

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Apache HTTP Server: 2.4 - 2.4.59

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Отказ в обслуживании

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://lists.apache.org/thread/zhzq56vjvz6610hycoj471gotljky894

Краткое описание: Выполнение произвольного кода в parse-server

Идентификатор уязвимости: CVE-2024-39309

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

Уязвимый продукт: parse-server: 6.5.0 - 7.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

31

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: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://github.com/parse-community/parse-server/security/advisories/GHSA-c2hr-cqg6-8j6r

32

Краткое описание: Выполнение произвольного кода в Netatalk

Идентификатор уязвимости: CVE-2024-38441

Идентификатор программной ошибки: CWE-193 Ошибка смещения на единицу

Уязвимый продукт: Netatalk: 2.4.0 - 3.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://github.com/Netatalk/netatalk/issues/1098
- http://github.com/Netatalk/netatalk/blob/90d91a9ac9a7d6132ab7620d31c8c23400949206/etc/afpd/directory.c#L2333
- http://github.com/Netatalk/netatalk/security/advisories/GHSA-mj6v-cr68-mj9q
- http://netatalk.io/security/CVE-2024-38441

33

Краткое описание: Выполнение произвольного кода в Netatalk

Идентификатор уязвимости: CVE-2024-38440

Идентификатор программной ошибки: CWE-193 Ошибка смещения на единицу

Уязвимый продукт: Netatalk: 2.4.0 - 3.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://github.com/Netatalk/netatalk/issues/1097
- http://github.com/Netatalk/netatalk/blob/90d91a9ac9a7d6132ab7620d31c8c23400949206/etc/uams/uams_dhx_pam.c#L199-L200
- http://github.com/Netatalk/netatalk/security/advisories/GHSA-mxx4-9fhm-r3w5
- http://netatalk.io/security/CVE-2024-38440
- https://bdu.fstec.ru/vul/2024-04823

34

Краткое описание: Выполнение произвольного кода в Netatalk

Идентификатор уязвимости: CVE-2024-38439

Идентификатор программной ошибки: CWE-193 Ошибка смещения на единицу

Уязвимый продукт: Netatalk: 2.4.0 - 3.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://github.com/Netatalk/netatalk/issues/1096
- http://github.com/Netatalk/netatalk/blob/90d91a9ac9a7d6132ab7620d31c8c23400949206/etc/uams/uams_pam.c#L316
- http://github.com/Netatalk/netatalk/security/advisories/GHSA-8r68-857c-4rqc
- http://netatalk.io/security/CVE-2024-38439

Краткое описание: Выполнение произвольного кода в OpenSSH

Идентификатор уязвимости: CVE-2024-6387

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: OpenSSH: 8.5p1 - 9.7p1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

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: 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: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://www.openssh.com/releasenotes.html#9.8p1
- http://seclists.org/oss-sec/2024/q3/2
- https://bdu.fstec.ru/vul/2024-04914

Краткое описание: Обход безопасности в Juniper Session Smart Router

Идентификатор уязвимости: CVE-2024-2973

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

Уязвимый продукт: Session Smart Router: до 6.2.5
Session Smart Conductor: до 6.2.5
WAN Assurance Router: до 6.2.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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: 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: 2024-07-01 / 2024-07-01

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-06-Out-Of-Cycle-Security-Bulletin-Session-Smart-Router-SSR-On-redundant-router-deployments-API-authentication-can-be-bypassed-CVE-2024-2973?language=en_US
- https://bdu.fstec.ru/vul/2024-04859