НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-07-22.1 | 22 июля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	None	Mitel Unify OpenScape 4000 and Unify OpenScape 4000 Manager	Сетевой	ACE	2024-07-22	✓
2	Высокая	CVE-2024-6600	Mozilla Thunderbird	Сетевой	ACE	2024-07-21	✓
3	Высокая	CVE-2024-6602	Mozilla Thunderbird	Сетевой	ACE	2024-07-21	✓
4	Высокая	CVE-2024-6604	Mozilla Thunderbird	Сетевой	ACE	2024-07-21	✓
5	Высокая	CVE-2024-6615	Mozilla Thunderbird	Сетевой	ACE	2024-07-21	✓
6	Критическая	CVE-2024-36039	PyMySQL	Сетевой	ACE	2024-07-18	✓
7	Критическая	CVE-2024-20419	Cisco Smart Software Manager On-Prem	Сетевой	OSI	2024-07-18	✓
8	Критическая	CVE-2024-6779	Google Chrome	Сетевой	ACE	2024-07-17	✓
9	Высокая	CVE-2024-6778	Google Chrome	Сетевой	ACE	2024-07-17	✓
10	Критическая	CVE-2024-6777	Google Chrome	Сетевой	ACE	2024-07-17	✓
11	Критическая	CVE-2024-6776	Google Chrome	Сетевой	ACE	2024-07-17	✓
12	Критическая	CVE-2024-6775	Google Chrome	Сетевой	ACE	2024-07-17	✓
13	Критическая	CVE-2024-6774	Google Chrome	Сетевой	ACE	2024-07-17	✓

14	Высокая	CVE-2024-6773	Google Chrome	Сетевой	ACE	2024-07-17	✓
15	Высокая	CVE-2024-6604	Mozilla Thunderbird 115	Сетевой	ACE	2024-07-16	✓
16	Высокая	CVE-2024-6602	Mozilla Thunderbird 115	Сетевой	ACE	2024-07-16	✓
17	Высокая	CVE-2024-6600	Mozilla Thunderbird 115	Сетевой	ACE	2024-07-16	✓
18	Критическая	CVE-2024-27349	Apache HugeGraph-Server	Сетевой	SB	2024-07-16	✓
19	Критическая	CVE-2024-27348	Apache HugeGraph-Server	Сетевой	ACE	2024-07-16	✓
20	Критическая	CVE-2024-5910	Palo Alto Networks Expedition	Сетевой	SB	2024-07-16	✓

1

Краткое описание: Выполнение произвольного кода в Mitel Unify OpenScape 4000 and Unify OpenScape 4000 Manager

Идентификатор уязвимости: None

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

Уязвимый продукт: Unify OpenScape 4000: 11 R0.22
Unify OpenScape 4000 Manager: 10 R1.34 - 11 R0.22

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: 2024-07-22 / 2024-07-22

Ссылки на источник:

- http://www.mitel.com/support/security-advisories/obso-2407-02

2

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-6600

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

Уязвимый продукт: Mozilla Thunderbird: 125.0 - 127.0

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: 2024-07-21 / 2024-07-21

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-32/

3

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-6602

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

Уязвимый продукт: Mozilla Thunderbird: 125.0 - 127.0

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: 2024-07-21 / 2024-07-21

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-32/

4

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-6604

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

Уязвимый продукт: Mozilla Thunderbird: 125.0 - 127.0

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: 2024-07-21 / 2024-07-21

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-32/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-6615

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

Уязвимый продукт: Mozilla Thunderbird: 125.0 - 127.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 2024-07-21 / 2024-07-21

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-32/

6

Краткое описание: Выполнение произвольного кода в PyMySQL

Идентификатор уязвимости: CVE-2024-36039
BDU:2024-04920

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

Уязвимый продукт: PyMySQL: 0.3 - 1.1.0

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: 2024-07-18 / 2024-07-18

Ссылки на источник:

- http://github.com/PyMySQL/PyMySQL/releases/tag/v1.1.1
- http://lists.debian.org/debian-lts-announce/2024/05/msg00017.html
- http://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/35VOJS3SRJNLQIO7YTZFNM6RWHIHWTMK/
- http://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/23VXBV34GFRICCVYZ6KFMSSWY5UEXCF5/
- https://bdu.fstec.ru/vul/2024-04920

7

Краткое описание: Получение конфиденциальной информации в Cisco Smart Software Manager On-Prem

Идентификатор уязвимости: CVE-2024-20419

Идентификатор программной ошибки: CWE-620 Смена пароля без подтверждения

Уязвимый продукт: Cisco Smart Software Manager On-Prem: 8-202206

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-18 / 2024-07-18

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy

8

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6779

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.127

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: 10.0 AV:N/AC:L/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: 2024-07-17 / 2024-07-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop.html
- http://crbug.com/351327767

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6778

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.127

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

9 **Рекомендации по устранению:** Данная уязвимость устраняется официальным 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: 2024-07-17 / 2024-07-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop.html
- http://crbug.com/341136300

10

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6777

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.127

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: 10.0 AV:N/AC:L/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: 2024-07-17 / 2024-07-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop.html
- http://crbug.com/345640549

11

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6776

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.127

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: 10.0 AV:N/AC:L/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: 2024-07-17 / 2024-07-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop.html
- http://crbug.com/346692546

12

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6775

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.127

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: 10.0 AV:N/AC:L/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: 2024-07-17 / 2024-07-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop.html
- http://crbug.com/347373236

13

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6774

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.127

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: 10.0 AV:N/AC:L/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: 2024-07-17 / 2024-07-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop.html
- http://crbug.com/346898524

14

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6773

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.127

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: 2024-07-17 / 2024-07-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop.html
- http://crbug.com/347724915

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird 115

Идентификатор уязвимости: CVE-2024-6604

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

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 115.12.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-07-16 / 2024-07-16

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-31/

16

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird 115

Идентификатор уязвимости: CVE-2024-6602

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

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 115.12.2

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: 2024-07-16 / 2024-07-16

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-31/

17

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird 115

Идентификатор уязвимости: CVE-2024-6600

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

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 115.12.2

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: 2024-07-16 / 2024-07-16

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-31/

18

Краткое описание: Обход безопасности в Apache HugeGraph-Server

Идентификатор уязвимости: CVE-2024-27349

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: HugeGraph-Server: 0.6.1 - 1.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2024-07-16 / 2024-07-16

Ссылки на источник:

- http://lists.apache.org/thread/dz9n9lndqfsf64t72o73r7sttrc6ocsd
- http://www.openwall.com/lists/oss-security/2024/04/22/4

Краткое описание: Выполнение произвольного кода в Apache HugeGraph-Server

Идентификатор уязвимости: CVE-2024-27348
BDU:2024-04433

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

Уязвимый продукт: HugeGraph-Server: 0.6.1 - 1.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

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:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-16 / 2024-07-16

Ссылки на источник:

- http://hugegraph.apache.org/docs/config/config-authentication/#configure-user-authentication
- http://lists.apache.org/thread/nx6g6htyhpgtzsocybm242781o8w5kq9
- http://www.openwall.com/lists/oss-security/2024/04/22/3
- https://bdu.fstec.ru/vul/2024-04433

Краткое описание: Обход безопасности в Palo Alto Networks Expedition

Идентификатор уязвимости: CVE-2024-5910

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

Уязвимый продукт: Expedition: до 1.2.92

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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: 2024-07-16 / 2024-07-16

Ссылки на источник:

- http://security.paloaltonetworks.com/CVE-2024-5910