НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-04-26.1 | 26 апреля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-31413	OMRON Sysmac Studio/CX-One and CX-Programmer	Сетевой	ACE	2024-04-25	✓
2	Высокая	CVE-2024-31412	OMRON Sysmac Studio/CX-One and CX-Programmer	Сетевой	DoS	2024-04-25	✓
3	Высокая	CVE-2024-20353	Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services	Сетевой	DoS	2024-04-24	✓
4	Высокая	CVE-2024-4058	Google Chrome	Сетевой	ACE	2024-04-24	✓
5	Высокая	CVE-2024-4060	Google Chrome	Сетевой	ACE	2024-04-24	✓
6	Критическая	CVE-2024-29889	GLPI	Сетевой	ACE	2024-04-24	✓
7	Высокая	CVE-2024-31456	GLPI	Сетевой	ACE	2024-04-24	✓
8	Высокая	CVE-2024-22254	Dell Custom VMware ESXi	Локальный	PE	2024-04-23	✓
9	Критическая	CVE-2024-22253	Dell Custom VMware ESXi	Локальный	ACE	2024-04-23	✓
10	Критическая	CVE-2024-22252	Dell Custom VMware ESXi	Локальный	ACE	2024-04-23	✓
11	Высокая	CVE-2024-29957	Brocade SANnav	Сетевой	OSI	2024-04-23	✓
12	Высокая	CVE-2024-29959	Brocade SANnav	Сетевой	OSI	2024-04-23	✓

13	Высокая	CVE-2024-29960	Brocade SANnav	Сетевой	OSI	2024-04-23	✓
14	Высокая	CVE-2024-29963	Brocade SANnav	Сетевой	OSI	2024-04-23	✓
15	Высокая	CVE-2024-29961	Brocade SANnav	Сетевой	OSI	2024-04-23	✓
16	Высокая	CVE-2024-29968	Brocade SANnav	Сетевой	OSI	2024-04-23	✓
17	Высокая	CVE-2024-29966	Brocade SANnav	Сетевой	OSI	2024-04-23	✓
18	Высокая	CVE-2024-29950	Brocade SANnav	Сетевой	OSI	2024-04-23	✓
19	Высокая	CVE-2024-29958	Brocade SANnav	Сетевой	OSI	2024-04-23	✓
20	Высокая	CVE-2024-28847	OpenMetadata	Сетевой	ACE	2024-04-22	✓
21	Высокая	CVE-2024-28848	OpenMetadata	Сетевой	ACE	2024-04-22	✓
22	Высокая	CVE-2024-28254	OpenMetadata	Сетевой	ACE	2024-04-22	✓
23	Критическая	CVE-2024-28255	OpenMetadata	Сетевой	SB	2024-04-22	✓
24	Критическая	CVE-2024-4040	CrushFTP	Сетевой	RLF	2024-04-22	✓
25	Высокая	CVE-2024-32477	Deno	Локальный	OSI	2024-04-22	✓

1

Краткое описание: Выполнение произвольного кода в OMRON Sysmac Studio/CX-One and CX-Programmer

Идентификатор уязвимости: CVE-2024-31413

Идентификатор программной ошибки: CWE-761 Освобождение указателя, находящегося не в начале буфера

Уязвимый продукт: CX-One: 4.61.1
Automation Software Sysmac Studio: 1.56

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 2024-04-25 / 2024-04-25

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU98274902/index.html
- http://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-002_en.pdf

2

Краткое описание: Отказ в обслуживании в OMRON Sysmac Studio/CX-One and CX-Programmer

Идентификатор уязвимости: CVE-2024-31412

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: CX-Programmer: 9.81

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2024-04-25 / 2024-04-25

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU98274902/index.html
- http://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-003_en.pdf

3

Краткое описание: Отказ в обслуживании в Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services

Идентификатор уязвимости: CVE-2024-20353

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

Уязвимый продукт: Cisco Adaptive Security Appliance (ASA): до 9.20.2.10
Cisco Firepower Threat Defense (FTD): до 9.20.2.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-24 / 2024-04-24

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwj10955
- http://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/
- https://bdu.fstec.ru/vul/2024-03233

4

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-4058

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 124.0.6367.62

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: 2024-04-24 / 2024-04-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_24.html
- http://issues.chromium.org/issues/332546345

5

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-4060

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 124.0.6367.62

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: 2024-04-24 / 2024-04-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_24.html
- http://crbug.com/333420620

6

Краткое описание: Выполнение произвольного кода в GLPI

Идентификатор уязвимости: CVE-2024-29889

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

Уязвимый продукт: GLPI: 10.0.0 - 10.0.14

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: 2024-04-24 / 2024-04-24

Ссылки на источник:

- http://github.com/glpi-project/glpi/releases/tag/10.0.15

Краткое описание: Выполнение произвольного кода в GLPI

Идентификатор уязвимости: CVE-2024-31456

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

Уязвимый продукт: GLPI: 10.0.0 - 10.0.14

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

7

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: 2024-04-24 / 2024-04-24

Ссылки на источник:

- http://github.com/glpi-project/glpi/releases/tag/10.0.15

8

Краткое описание: Повышение привилегий в Dell Custom VMware ESXi

Идентификатор уязвимости: CVE-2024-22254

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Dell custom VMware ESXi: до 8.0U2-A06

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.9 AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224179/dsa-2024-182-security-update-for-dell-custom-vmware-esxi-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01810

9

Краткое описание: Выполнение произвольного кода в Dell Custom VMware ESXi

Идентификатор уязвимости: CVE-2024-22253

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Dell custom VMware ESXi: до 8.0U2-A06

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224179/dsa-2024-182-security-update-for-dell-custom-vmware-esxi-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01808

10

Краткое описание: Выполнение произвольного кода в Dell Custom VMware ESXi

Идентификатор уязвимости: CVE-2024-22252

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Dell custom VMware ESXi: до 8.0U2-A06

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224179/dsa-2024-182-security-update-for-dell-custom-vmware-esxi-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01807

Краткое описание: Получение конфиденциальной информации в Brocade SANnav

Идентификатор уязвимости: CVE-2024-29957

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

Уязвимый продукт: Brocade SANnav: до 2.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://support.broadcom.com/external/content/SecurityAdvisories/0/23241

Краткое описание: Получение конфиденциальной информации в Brocade SANnav

Идентификатор уязвимости: CVE-2024-29959

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

Уязвимый продукт: Brocade SANnav: до 2.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://support.broadcom.com/external/content/SecurityAdvisories/0/23243

13

Краткое описание: Получение конфиденциальной информации в Brocade SANnav

Идентификатор уязвимости: CVE-2024-29960

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

Уязвимый продукт: Brocade SANnav: до 2.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 7.5 AV: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: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://support.broadcom.com/external/content/SecurityAdvisories/0/23244

Краткое описание: Получение конфиденциальной информации в Brocade SANnav

Идентификатор уязвимости: CVE-2024-29963

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: Brocade SANnav: до 2.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://support.broadcom.com/external/content/SecurityAdvisories/0/23247

Краткое описание: Получение конфиденциальной информации в Brocade SANnav

Идентификатор уязвимости: CVE-2024-29961

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

Уязвимый продукт: Brocade SANnav: до 2.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://support.broadcom.com/external/content/SecurityAdvisories/0/23246

16

Краткое описание: Получение конфиденциальной информации в Brocade SANnav

Идентификатор уязвимости: CVE-2024-29968

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

Уязвимый продукт: Brocade SANnav: до 2.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://support.broadcom.com/external/content/SecurityAdvisories/0/23253

17

Краткое описание: Получение конфиденциальной информации в Brocade SANnav

Идентификатор уязвимости: CVE-2024-29966

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

Уязвимый продукт: Brocade SANnav: до 2.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование жестко закодированных учетных данных

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: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://support.broadcom.com/external/content/SecurityAdvisories/0/23255

18

Краткое описание: Получение конфиденциальной информации в Brocade SANnav

Идентификатор уязвимости: CVE-2024-29950

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Brocade SANnav: до 2.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 7.5 AV: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: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://support.broadcom.com/external/content/SecurityAdvisories/0/23236

19

Краткое описание: Получение конфиденциальной информации в Brocade SANnav

Идентификатор уязвимости: CVE-2024-29958

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

Уязвимый продукт: Brocade SANnav: до 2.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 7.5 AV: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: 2024-04-23 / 2024-04-23

Ссылки на источник:

- http://support.broadcom.com/external/content/SecurityAdvisories/0/23242

Краткое описание: Выполнение произвольного кода в OpenMetadata

Идентификатор уязвимости: CVE-2024-28847

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

Уязвимый продукт: OpenMetadata: 0.3.0 - 1.2.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

20 **Вектор атаки:** Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-22 / 2024-04-22

Ссылки на источник:

- http://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-8p5r-6mvv-2435
- http://codeql.github.com/codeql-query-help/java/java-spel-expression-injection
- http://github.com/open-metadata/OpenMetadata/blob/b6b337e09a05101506a5faba4b45d370cc3c9fc8/openmetadata-service/src/main/java/org/openmetadata/service/jdbi3/EntityRepository.java#L693
- http://github.com/open-metadata/OpenMetadata/blob/b6b337e09a05101506a5faba4b45d370cc3c9fc8/openmetadata-service/src/main/java/org/openmetadata/service/jdbi3/EventSubscriptionRepository.java#L69-L83
- http://github.com/open-metadata/OpenMetadata/blob/b6b337e09a05101506a5faba4b45d370cc3c9fc8/openmetadata-service/src/main/java/org/openmetadata/service/resources/EntityResource.java#L219
- http://github.com/open-metadata/OpenMetadata/blob/b6b337e09a05101506a5faba4b45d370cc3c9fc8/openmetadata-service/src/main/java/org/openmetadata/service/resources/events/subscription/EventSubscriptionResource.java#L289

21

Краткое описание: Выполнение произвольного кода в OpenMetadata

Идентификатор уязвимости: CVE-2024-28848

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

Уязвимый продукт: OpenMetadata: 0.3.0 - 1.2.3

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2024-04-22 / 2024-04-22

Ссылки на источник:

- http://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-5xv3-fm7g-865r
- http://codeql.github.com/codeql-query-help/java/java-spel-expression-injection
- http://github.com/open-metadata/OpenMetadata/blob/main/openmetadata-service/src/main/java/org/openmetadata/service/security/policyevaluator/CompiledRule.java#L51
- http://github.com/open-metadata/OpenMetadata/blob/main/openmetadata-service/src/main/java/org/openmetadata/service/security/policyevaluator/CompiledRule.java#L57

Краткое описание: Выполнение произвольного кода в OpenMetadata

Идентификатор уязвимости: CVE-2024-28254

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

Уязвимый продукт: OpenMetadata: 0.3.0 - 1.2.3

Категория уязвимого продукта: Серверное программное обеспечение и его 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.

22

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: 2024-04-22 / 2024-04-22

Ссылки на источник:

- http://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-j86m-rrpr-g8gw
- http://codeql.github.com/codeql-query-help/java/java-spel-expression-injection
- http://github.com/open-metadata/OpenMetadata/blob/84054a85d3478e3e3795fe92daa633ec11c9d6d9/openmetadata-service/src/main/java/org/openmetadata/service/events/subscription/AlertUtil.java#L101
- http://github.com/open-metadata/OpenMetadata/blob/84054a85d3478e3e3795fe92daa633ec11c9d6d9/openmetadata-service/src/main/java/org/openmetadata/service/events/subscription/AlertUtil.java#L108
- http://github.com/spring-projects/spring-framework/blob/4e2d3573189b7c0afce62bce29cd915de4077f56/spring-expression/src/main/java/org/springframework/expression/spel/standard/SpelExpression.java#L106

23

Краткое описание: Обход безопасности в OpenMetadata

Идентификатор уязвимости: CVE-2024-28255

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: OpenMetadata: 0.3.0 - 1.2.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-22 / 2024-04-22

Ссылки на источник:

- http://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-6wx7-qw5p-wh84
- http://github.com/open-metadata/OpenMetadata/blob/e2043a3f31312ebb42391d6c93a67584d798de52/openmetadata-service/src/main/java/org/openmetadata/service/security/JwtFilter.java#L111
- http://github.com/open-metadata/OpenMetadata/blob/e2043a3f31312ebb42391d6c93a67584d798de52/openmetadata-service/src/main/java/org/openmetadata/service/security/JwtFilter.java#L113
- https://bdu.fstec.ru/vul/2024-03058

Краткое описание: Чтение локальных файлов в CrushFTP

Идентификатор уязвимости: CVE-2024-4040

Идентификатор программной ошибки: CWE-73 Внешнее управление именем или путем файла

Уязвимый продукт: CrushFTP: до 11.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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.

24

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: 2024-04-22 / 2024-04-22

Ссылки на источник:

- http://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update
- http://old.reddit.com/r/crowdstrike/comments/1c88788/situational_awareness_20240419_crushftp_virtual/
- http://crushftp.com/version11_build.html
- https://bdu.fstec.ru/vul/2024-03173

Краткое описание: Получение конфиденциальной информации в Deno

Идентификатор уязвимости: CVE-2024-32477

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

Уязвимый продукт: Deno: 1.42.0 - 1.42.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

25

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

Оценка CVSSv3: 7.7 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-22 / 2024-04-22

Ссылки на источник:

- http://github.com/denoland/deno/security/advisories/GHSA-95cj-3hr2-7j5j