НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-09-09.1 | 9 сентября 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-6779	Google ChromeOS	Сетевой	ACE	2024-09-09	✓
2	Высокая	CVE-2024-7965	Google ChromeOS	Сетевой	OSI	2024-09-09	✓
3	Критическая	CVE-2024-8387	Mozilla Thunderbird	Сетевой	ACE	2024-09-09	✓
4	Критическая	CVE-2024-8384	Mozilla Thunderbird	Сетевой	ACE	2024-09-09	✓
5	Высокая	CVE-2024-8383	Mozilla Thunderbird	Сетевой	OSI	2024-09-09	✓
6	Высокая	CVE-2024-8382	Mozilla Thunderbird	Сетевой	OSI	2024-09-09	✓
7	Критическая	CVE-2024-8381	Mozilla Thunderbird	Сетевой	ACE	2024-09-09	✓
8	Критическая	CVE-2024-8385	Mozilla Thunderbird	Сетевой	ACE	2024-09-09	✓
9	Критическая	CVE-2024-38650	Veeam Service Provider Console	Сетевой	OSI	2024-09-06	✓
10	Критическая	CVE-2024-39714	Veeam Service Provider Console	Сетевой	WLF	2024-09-06	✓
11	Высокая	CVE-2024-39715	Veeam Service Provider Console	Сетевой	WLF	2024-09-06	✓
12	Высокая	CVE-2024-38651	Veeam Service Provider Console	Сетевой	WLF	2024-09-06	✓
13	Критическая	CVE-2024-44383	WAYOS FBM-291W	Сетевой	ACE	2024-09-06	✗

14	Высокая	CVE-2024-45287	FreeBSD	Сетевой	ACE	2024-09-06	✓
15	Критическая	CVE-2024-45288	FreeBSD	Сетевой	ACE	2024-09-06	✓
16	Критическая	CVE-2024-35306	Pandora FMS	Сетевой	ACE	2024-09-06	✓
17	Критическая	CVE-2024-35305	Pandora FMS	Сетевой	ACE	2024-09-06	✓
18	Критическая	CVE-2024-37285	Elastic Kibana	Сетевой	ACE	2024-09-06	✓
19	Критическая	CVE-2024-37288	Elastic Kibana	Сетевой	ACE	2024-09-06	✓
20	Высокая	CVE-2024-38875	Ansible Automation Platform 2.4 packages	Сетевой	DoS	2024-09-06	✓
21	Высокая	CVE-2024-39329	Ansible Automation Platform 2.4 packages	Сетевой	OSI	2024-09-06	✓
22	Высокая	CVE-2024-39330	Ansible Automation Platform 2.4 packages	Сетевой	RLF	2024-09-06	✓
23	Высокая	CVE-2024-41989	Ansible Automation Platform 2.4 packages	Сетевой	DoS	2024-09-06	✓
24	Высокая	CVE-2024-41990	Ansible Automation Platform 2.4 packages	Сетевой	DoS	2024-09-06	✓
25	Высокая	CVE-2024-41991	Ansible Automation Platform 2.4 packages	Сетевой	DoS	2024-09-06	✓
26	Критическая	CVE-2024-42005	Ansible Automation Platform 2.4 packages	Сетевой	ACE	2024-09-06	✓

27	Критическая	CVE-2024-39705	Python NLTK library	Сетевой	ACE	2024-09-05	✓
28	Высокая	CVE-2024-42491	Asterisk	Сетевой	DoS	2024-09-05	✓
29	Высокая	CVE-2024-7885	Undertow	Сетевой	OSI	2024-09-05	✓
30	Критическая	CVE-2024-44400	D-Link DI-8400	Сетевой	ACE	2024-09-05	✗
31	Высокая	CVE-2024-45506	HAProxy	Сетевой	DoS	2024-09-05	✓
32	Критическая	CVE-2024-45510	Zimbra Collaboration	Сетевой	XSS\CSS	2024-09-04	✓
33	Критическая	CVE-2024-45518	Zimbra Collaboration	Сетевой	CSRF	2024-09-04	✓
34	Критическая	CVE-2024-45519	Zimbra Collaboration	Сетевой	ACE	2024-09-04	✓
35	Высокая	CVE-2024-20440	Cisco Smart Licensing Utility	Сетевой	OSI	2024-09-04	✓
36	Критическая	CVE-2024-20439	Cisco Smart Licensing Utility	Сетевой	ACE	2024-09-04	✓
37	Критическая	CVE-2024-44342	D-Link DIR-846W	Сетевой	ACE	2024-09-04	✗
38	Критическая	CVE-2024-44341	D-Link DIR-846W	Сетевой	ACE	2024-09-04	✗
39	Высокая	CVE-2024-44340	D-Link DIR-846W	Сетевой	ACE	2024-09-04	✗
40	Критическая	CVE-2024-41622	D-Link DIR-846W	Сетевой	ACE	2024-09-04	✗
41	Высокая	CVE-2024-22273	VMware ESXi, Cloud Foundation, VMware Fusion, VMware Workstation	Локальный	ACE	2024-09-04	✓

1

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-6779
BDU:2024-06113

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

Уязвимый продукт: Chrome OS: до 126.0.6478.252

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-09-09 / 2024-09-09

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for_6.html
- https://bdu.fstec.ru/vul/2024-06113

2

Краткое описание: Получение конфиденциальной информации в Google ChromeOS

Идентификатор уязвимости: CVE-2024-7965

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

Уязвимый продукт: Chrome OS: до 126.0.6478.252

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

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for_6.html

3

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-8387
BDU:2024-06697

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

Уязвимый продукт: Mozilla Thunderbird: 128.0 - 128.1.1

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: 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: 2024-09-09 / 2024-09-09

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-43/
- https://bdu.fstec.ru/vul/2024-06697

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-8384
BDU:2024-06703

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

Уязвимый продукт: Mozilla Thunderbird: 128.0 - 128.1.1

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-09-09 / 2024-09-09

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-43/
- https://bdu.fstec.ru/vul/2024-06703

Краткое описание: Получение конфиденциальной информации в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-8383
BDU:2024-06700

Идентификатор программной ошибки: CWE-939 Некорректная авторизация в обработчике нестандартных схем URL

Уязвимый продукт: Mozilla Thunderbird: 128.0 - 128.1.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-43/
- https://bdu.fstec.ru/vul/2024-06700

6

Краткое описание: Получение конфиденциальной информации в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-8382
BDU:2024-06698

Идентификатор программной ошибки: CWE-749 Доступны опасные методы или функции

Уязвимый продукт: Mozilla Thunderbird: 128.0 - 128.1.1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-43/
- https://bdu.fstec.ru/vul/2024-06698

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-8381
BDU:2024-06699

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

Уязвимый продукт: Mozilla Thunderbird: 128.0 - 128.1.1

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-09-09 / 2024-09-09

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-43/
- https://bdu.fstec.ru/vul/2024-06699

8

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-8385
BDU:2024-06731

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

Уязвимый продукт: Mozilla Thunderbird: 128.0 - 128.1.1

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: 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: 2024-09-09 / 2024-09-09

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-43/
- https://bdu.fstec.ru/vul/2024-06731

Краткое описание: Получение конфиденциальной информации в Veeam Service Provider Console

Идентификатор уязвимости: CVE-2024-38650

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Veeam Service Provider Console: 7.0.0.12777 - 8.0.0.19552

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://www.veeam.com/kb4649

10

Краткое описание: Запись локальных файлов в Veeam Service Provider Console

Идентификатор уязвимости: CVE-2024-39714

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

Уязвимый продукт: Veeam Service Provider Console: 7.0.0.12777 - 8.0.0.19552

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://www.veeam.com/kb4649

Краткое описание: Запись локальных файлов в Veeam Service Provider Console

Идентификатор уязвимости: CVE-2024-39715

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

Уязвимый продукт: Veeam Service Provider Console: 7.0.0.12777 - 8.0.0.19552

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://www.veeam.com/kb4649

12

Краткое описание: Запись локальных файлов в Veeam Service Provider Console

Идентификатор уязвимости: CVE-2024-38651

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

Уязвимый продукт: Veeam Service Provider Console: 7.0.0.12777 - 8.0.0.19552

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://www.veeam.com/kb4649

13

Краткое описание: Выполнение произвольного кода в WAYOS FBM-291W

Идентификатор уязвимости: CVE-2024-44383

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

Уязвимый продукт: FBM-291W: 19.09.11

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

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/E:P/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://github.com/GroundCTL2MajorTom/pocs/blob/main/wayos_%20FBM_291W.md

Краткое описание: Выполнение произвольного кода в FreeBSD

Идентификатор уязвимости: CVE-2024-45287

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

Уязвимый продукт: FreeBSD: до 14.1

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://security.freebsd.org/advisories/FreeBSD-SA-24:09.libnv.asc

Краткое описание: Выполнение произвольного кода в FreeBSD

Идентификатор уязвимости: CVE-2024-45288

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FreeBSD: до 14.1

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

Способ эксплуатации: Не определено

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: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://security.freebsd.org/advisories/FreeBSD-SA-24:09.libnv.asc

Краткое описание: Выполнение произвольного кода в Pandora FMS

Идентификатор уязвимости: CVE-2024-35306
BDU:2024-04832

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

Уязвимый продукт: Pandora FMS: 700 - 776

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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: 9.1 AV:N/AC:L/PR:H/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: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://pandorafms.com/en/security/common-vulnerabilities-and-exposures/
- https://bdu.fstec.ru/vul/2024-04832

Краткое описание: Выполнение произвольного кода в Pandora FMS

Идентификатор уязвимости: CVE-2024-35305

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

Уязвимый продукт: Pandora FMS: 700 - 776

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://pandorafms.com/en/security/common-vulnerabilities-and-exposures/

Краткое описание: Выполнение произвольного кода в Elastic Kibana

Идентификатор уязвимости: CVE-2024-37285

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Kibana: 8.10.0 - 8.15.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://discuss.elastic.co/t/kibana-8-15-1-security-update-esa-2024-27-esa-2024-28/366119

Краткое описание: Выполнение произвольного кода в Elastic Kibana

Идентификатор уязвимости: CVE-2024-37288

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Kibana: 8.15.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://discuss.elastic.co/t/kibana-8-15-1-security-update-esa-2024-27-esa-2024-28/366119

20

Краткое описание: Отказ в обслуживании в Ansible Automation Platform 2.4 packages

Идентификатор уязвимости: CVE-2024-38875

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: python3x-pulpcore (Red Hat package): до 3.28.31-1.el8ap
python3x-pulp-ansible (Red Hat package): до 0.20.8-1.el8ap
python3x-jmespath (Red Hat package): до 0.10.0-5.el8ap
python3x-gunicorn (Red Hat package): до 22.0.0-2.el8ap
python3x-grpcio (Red Hat package): до 1.58.3-1.el8ap
python3x-django (Red Hat package): до 4.2.15-1.el8ap
python-zipp (Red Hat package): до 3.19.2-1.el9ap
python-pulpcore (Red Hat package): до 3.28.31-1.el9ap
python-pulp-ansible (Red Hat package): до 0.20.8-1.el9ap
python-jmespath (Red Hat package): до 0.10.0-5.el9ap
python-gunicorn (Red Hat package): до 22.0.0-2.el9ap
python-grpcio (Red Hat package): до 1.58.3-1.el9ap
python-django (Red Hat package): до 4.2.15-1.el9ap
automation-controller (Red Hat package): до 4.5.10-1.el9ap
Ansible Automation Platform: до 2.4

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2024:6428

21

Краткое описание: Получение конфиденциальной информации в Ansible Automation Platform 2.4 packages

Идентификатор уязвимости: CVE-2024-39329

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

Уязвимый продукт: python3x-pulpcore (Red Hat package): до 3.28.31-1.el8ap
python3x-pulp-ansible (Red Hat package): до 0.20.8-1.el8ap
python3x-jmespath (Red Hat package): до 0.10.0-5.el8ap
python3x-gunicorn (Red Hat package): до 22.0.0-2.el8ap
python3x-grpcio (Red Hat package): до 1.58.3-1.el8ap
python3x-django (Red Hat package): до 4.2.15-1.el8ap
python-zipp (Red Hat package): до 3.19.2-1.el9ap
python-pulpcore (Red Hat package): до 3.28.31-1.el9ap
python-pulp-ansible (Red Hat package): до 0.20.8-1.el9ap
python-jmespath (Red Hat package): до 0.10.0-5.el9ap
python-gunicorn (Red Hat package): до 22.0.0-2.el9ap
python-grpcio (Red Hat package): до 1.58.3-1.el9ap
python-django (Red Hat package): до 4.2.15-1.el9ap
automation-controller (Red Hat package): до 4.5.10-1.el9ap
Ansible Automation Platform: до 2.4

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2024:6428

22

Краткое описание: Чтение локальных файлов в Ansible Automation Platform 2.4 packages

Идентификатор уязвимости: CVE-2024-39330

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

Уязвимый продукт: python3x-pulpcore (Red Hat package): до 3.28.31-1.el8ap
python3x-pulp-ansible (Red Hat package): до 0.20.8-1.el8ap
python3x-jmespath (Red Hat package): до 0.10.0-5.el8ap
python3x-gunicorn (Red Hat package): до 22.0.0-2.el8ap
python3x-grpcio (Red Hat package): до 1.58.3-1.el8ap
python3x-django (Red Hat package): до 4.2.15-1.el8ap
python-zipp (Red Hat package): до 3.19.2-1.el9ap
python-pulpcore (Red Hat package): до 3.28.31-1.el9ap
python-pulp-ansible (Red Hat package): до 0.20.8-1.el9ap
python-jmespath (Red Hat package): до 0.10.0-5.el9ap
python-gunicorn (Red Hat package): до 22.0.0-2.el9ap
python-grpcio (Red Hat package): до 1.58.3-1.el9ap
python-django (Red Hat package): до 4.2.15-1.el9ap
automation-controller (Red Hat package): до 4.5.10-1.el9ap
Ansible Automation Platform: до 2.4

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2024:6428

23

Краткое описание: Отказ в обслуживании в Ansible Automation Platform 2.4 packages

Идентификатор уязвимости: CVE-2024-41989

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

Уязвимый продукт: python3x-pulpcore (Red Hat package): до 3.28.31-1.el8ap
python3x-pulp-ansible (Red Hat package): до 0.20.8-1.el8ap
python3x-jmespath (Red Hat package): до 0.10.0-5.el8ap
python3x-gunicorn (Red Hat package): до 22.0.0-2.el8ap
python3x-grpcio (Red Hat package): до 1.58.3-1.el8ap
python3x-django (Red Hat package): до 4.2.15-1.el8ap
python-zipp (Red Hat package): до 3.19.2-1.el9ap
python-pulpcore (Red Hat package): до 3.28.31-1.el9ap
python-pulp-ansible (Red Hat package): до 0.20.8-1.el9ap
python-jmespath (Red Hat package): до 0.10.0-5.el9ap
python-gunicorn (Red Hat package): до 22.0.0-2.el9ap
python-grpcio (Red Hat package): до 1.58.3-1.el9ap
python-django (Red Hat package): до 4.2.15-1.el9ap
automation-controller (Red Hat package): до 4.5.10-1.el9ap
Ansible Automation Platform: до 2.4

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

Способ эксплуатации: Не определено

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: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2024:6428

24

Краткое описание: Отказ в обслуживании в Ansible Automation Platform 2.4 packages

Идентификатор уязвимости: CVE-2024-41990

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: python3x-pulpcore (Red Hat package): до 3.28.31-1.el8ap
python3x-pulp-ansible (Red Hat package): до 0.20.8-1.el8ap
python3x-jmespath (Red Hat package): до 0.10.0-5.el8ap
python3x-gunicorn (Red Hat package): до 22.0.0-2.el8ap
python3x-grpcio (Red Hat package): до 1.58.3-1.el8ap
python3x-django (Red Hat package): до 4.2.15-1.el8ap
python-zipp (Red Hat package): до 3.19.2-1.el9ap
python-pulpcore (Red Hat package): до 3.28.31-1.el9ap
python-pulp-ansible (Red Hat package): до 0.20.8-1.el9ap
python-jmespath (Red Hat package): до 0.10.0-5.el9ap
python-gunicorn (Red Hat package): до 22.0.0-2.el9ap
python-grpcio (Red Hat package): до 1.58.3-1.el9ap
python-django (Red Hat package): до 4.2.15-1.el9ap
automation-controller (Red Hat package): до 4.5.10-1.el9ap
Ansible Automation Platform: до 2.4

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2024:6428

25

Краткое описание: Отказ в обслуживании в Ansible Automation Platform 2.4 packages

Идентификатор уязвимости: CVE-2024-41991

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: python3x-pulpcore (Red Hat package): до 3.28.31-1.el8ap
python3x-pulp-ansible (Red Hat package): до 0.20.8-1.el8ap
python3x-jmespath (Red Hat package): до 0.10.0-5.el8ap
python3x-gunicorn (Red Hat package): до 22.0.0-2.el8ap
python3x-grpcio (Red Hat package): до 1.58.3-1.el8ap
python3x-django (Red Hat package): до 4.2.15-1.el8ap
python-zipp (Red Hat package): до 3.19.2-1.el9ap
python-pulpcore (Red Hat package): до 3.28.31-1.el9ap
python-pulp-ansible (Red Hat package): до 0.20.8-1.el9ap
python-jmespath (Red Hat package): до 0.10.0-5.el9ap
python-gunicorn (Red Hat package): до 22.0.0-2.el9ap
python-grpcio (Red Hat package): до 1.58.3-1.el9ap
python-django (Red Hat package): до 4.2.15-1.el9ap
automation-controller (Red Hat package): до 4.5.10-1.el9ap
Ansible Automation Platform: до 2.4

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2024:6428

26

Краткое описание: Выполнение произвольного кода в Ansible Automation Platform 2.4 packages

Идентификатор уязвимости: CVE-2024-42005
BDU:2024-06269

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

Уязвимый продукт: python3x-pulpcore (Red Hat package): до 3.28.31-1.el8ap
python3x-pulp-ansible (Red Hat package): до 0.20.8-1.el8ap
python3x-jmespath (Red Hat package): до 0.10.0-5.el8ap
python3x-gunicorn (Red Hat package): до 22.0.0-2.el8ap
python3x-grpcio (Red Hat package): до 1.58.3-1.el8ap
python3x-django (Red Hat package): до 4.2.15-1.el8ap
python-zipp (Red Hat package): до 3.19.2-1.el9ap
python-pulpcore (Red Hat package): до 3.28.31-1.el9ap
python-pulp-ansible (Red Hat package): до 0.20.8-1.el9ap
python-jmespath (Red Hat package): до 0.10.0-5.el9ap
python-gunicorn (Red Hat package): до 22.0.0-2.el9ap
python-grpcio (Red Hat package): до 1.58.3-1.el9ap
python-django (Red Hat package): до 4.2.15-1.el9ap
automation-controller (Red Hat package): до 4.5.10-1.el9ap
Ansible Automation Platform: до 2.4

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 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: 2024-09-06 / 2024-09-06

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2024:6428
- https://bdu.fstec.ru/vul/2024-06269

27

Краткое описание: Выполнение произвольного кода в Python NLTK library

Идентификатор уязвимости: CVE-2024-39705

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Natural Language Toolkit: 2.0.1 - 3.8.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-09-05 / 2024-09-05

Ссылки на источник:

- http://github.com/nltk/nltk/issues/3266
- http://github.com/nltk/nltk/issues/2522
- http://www.vicarius.io/vsociety/posts/rce-in-python-nltk-cve-2024-39705-39706

Краткое описание: Отказ в обслуживании в Asterisk

Идентификатор уязвимости: CVE-2024-42491
BDU:2024-06734

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Certified Asterisk: 18.9-cert1 - 20.7-cert2
Asterisk Open Source: 18.0.0 rc1 - 21.4.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

28

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: 2024-09-05 / 2024-09-05

Ссылки на источник:

- http://github.com/asterisk/asterisk/security/advisories/GHSA-v428-g3cw-7hv9
- https://bdu.fstec.ru/vul/2024-06734

29

Краткое описание: Получение конфиденциальной информации в Undertow

Идентификатор уязвимости: CVE-2024-7885

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

Уязвимый продукт: Undertow: 2.0.0 - 2.3.16

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-05 / 2024-09-05

Ссылки на источник:

- http://access.redhat.com/security/cve/CVE-2024-7885
- http://bugzilla.redhat.com/show_bug.cgi?id=2305290

Краткое описание: Выполнение произвольного кода в D-Link DI-8400

Идентификатор уязвимости: CVE-2024-44400

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

Уязвимый продукт: DI-8400: 16.07.26A1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

30

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: 2024-09-05 / 2024-09-05

Ссылки на источник:

- http://github.com/lonelylonglong/openfile-/blob/main/D-link_DI_8400-16.07.26A1_Command_Injection.md/D-link_DI_8400-16.07.26A1_Command_Injection.md

31

Краткое описание: Отказ в обслуживании в HAProxy

Идентификатор уязвимости: CVE-2024-45506
BDU:2024-06744

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

Уязвимый продукт: HAProxy: 2.9.0 - 3.0.3

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

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: 2024-09-05 / 2024-09-05

Ссылки на источник:

- http://www.haproxy.org/download/3.1/src/CHANGELOG
- http://www.mail-archive.com/haproxy%40formilux.org/msg45281.html
- http://www.mail-archive.com/haproxy%40formilux.org/msg45280.html
- http://git.haproxy.org/?p=haproxy-3.0.git%3Ba=commitdiff%3Bh=c725db17e8416ffb3c1537aea756356228ce5e3c
- http://git.haproxy.org/?p=haproxy-3.0.git%3Ba=commitdiff%3Bh=d636e515453320c6e122c313c661a8ac7d387c7f
- https://bdu.fstec.ru/vul/2024-06744

Краткое описание: Межсайтовый скриптинг в Zimbra Collaboration

Идентификатор уязвимости: CVE-2024-45510

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

Уязвимый продукт: Zimbra Collaboration: 9.0.0 - 10.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Межсайтовый скриптинг

32

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-04 / 2024-09-04

Ссылки на источник:

- http://wiki.zimbra.com/wiki/Security_Center#ZCS_9.0.0_Patch_41_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_10.0.9_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_10.1.1_Released

33

Краткое описание: Подделка запросов на стороне сервера в Zimbra Collaboration

Идентификатор уязвимости: CVE-2024-45518

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

Уязвимый продукт: Zimbra Collaboration: 8.8.15 - 10.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Подделка запросов на стороне сервера

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:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-04 / 2024-09-04

Ссылки на источник:

- http://wiki.zimbra.com/wiki/Security_Center#ZCS_9.0.0_Patch_41_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_8.8.15_Patch_46_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_10.0.9_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_10.1.1_Released

34

Краткое описание: Выполнение произвольного кода в Zimbra Collaboration

Идентификатор уязвимости: CVE-2024-45519

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

Уязвимый продукт: Zimbra Collaboration: 8.8.15 - 10.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-04 / 2024-09-04

Ссылки на источник:

- http://wiki.zimbra.com/wiki/Security_Center#ZCS_9.0.0_Patch_41_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_8.8.15_Patch_46_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_10.0.9_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_10.1.1_Released

35

Краткое описание: Получение конфиденциальной информации в Cisco Smart Licensing Utility

Идентификатор уязвимости: CVE-2024-20440
BDU:2024-06720

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

Уязвимый продукт: Cisco Smart Licensing Utility: 2.0.0 - 2.2.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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: 2024-09-04 / 2024-09-04

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwi47950
- https://bdu.fstec.ru/vul/2024-06720

36

Краткое описание: Выполнение произвольного кода в Cisco Smart Licensing Utility

Идентификатор уязвимости: CVE-2024-20439
BDU:2024-06721

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: Cisco Smart Licensing Utility: 2.0.0 - 2.2.0

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 2024-09-04 / 2024-09-04

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwi41731
- https://bdu.fstec.ru/vul/2024-06721

Краткое описание: Выполнение произвольного кода в D-Link DIR-846W

Идентификатор уязвимости: CVE-2024-44342
BDU:2024-06740

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

Уязвимый продукт: DIR-846W: A1 FW100A43

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

37 **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: 2024-09-04 / 2024-09-04

Ссылки на источник:

- http://www.dlink.com/en/security-bulletin/
- http://www.dlink.com.cn/techsupport/ProductInfo.aspx?m=DIR-846W
- http://github.com/yali-1002/some-poc/blob/main/CVE-2024-44342
- https://bdu.fstec.ru/vul/2024-06740

Краткое описание: Выполнение произвольного кода в D-Link DIR-846W

Идентификатор уязвимости: CVE-2024-44341
BDU:2024-06739

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

Уязвимый продукт: DIR-846W: A1 FW100A43

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

38 **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: 2024-09-04 / 2024-09-04

Ссылки на источник:

- http://www.dlink.com/en/security-bulletin/
- http://www.dlink.com.cn/techsupport/ProductInfo.aspx?m=DIR-846W
- http://github.com/yali-1002/some-poc/blob/main/CVE-2024-44341
- https://bdu.fstec.ru/vul/2024-06739

Краткое описание: Выполнение произвольного кода в D-Link DIR-846W

Идентификатор уязвимости: CVE-2024-44340
BDU:2024-06588

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

Уязвимый продукт: DIR-846W: A1 FW100A43

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2024-09-04 / 2024-09-04

Ссылки на источник:

- http://www.dlink.com/en/security-bulletin/
- http://www.dlink.com.cn/techsupport/ProductInfo.aspx?m=DIR-846W
- http://github.com/yali-1002/some-poc/blob/main/CVE-2024-44340
- https://bdu.fstec.ru/vul/2024-06588

Краткое описание: Выполнение произвольного кода в D-Link DIR-846W

Идентификатор уязвимости: CVE-2024-41622

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

Уязвимый продукт: DIR-846W: A1 FW100A43

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

40 **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: 2024-09-04 / 2024-09-04

Ссылки на источник:

- http://www.dlink.com/en/security-bulletin/
- http://www.dlink.com.cn/techsupport/ProductInfo.aspx?m=DIR-846W
- http://github.com/yali-1002/some-poc/blob/main/CVE-2024-41622

41

Краткое описание: Выполнение произвольного кода в VMware ESXi, Cloud Foundation, VMware Fusion, VMware Workstation

Идентификатор уязвимости: CVE-2024-22273
BDU:2024-04135

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: VMware ESXi: ESXi70U1b-17168206 - ESXi80U1d-23299997
Cloud Foundation: до 5.1.1
VMware Fusion: 13.0 - 13.5
VMware Workstation: 17.0 - 17.5

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-04 / 2024-09-04

Ссылки на источник:

- http://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24308
- https://bdu.fstec.ru/vul/2024-04135