

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2024-10-21.1 | 21 октября 2024 года

TLP: WHITE



Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-48904	Trend Micro Cloud Edge REST API	Сетевой	ACE	2024-10-18	✓
2	Высокая	CVE-2024-36387	cPanel EasyApache	Сетевой	DoS	2024-10-17	✓
3	Высокая	CVE-2024-36138	cPanel EasyApache	Сетевой	OSI	2024-10-17	✓
4	Высокая	CVE-2024-38475	cPanel EasyApache	Сетевой	ACE	2024-10-17	✓
5	Критическая	CVE-2024-38476	cPanel EasyApache	Сетевой	CSRF	2024-10-17	✓
6	Высокая	CVE-2024-38477	cPanel EasyApache	Сетевой	DoS	2024-10-17	✓
7	Высокая	CVE-2024-8927	cPanel EasyApache	Сетевой	SB	2024-10-17	✓
8	Высокая	CVE-2024-8926	cPanel EasyApache	Сетевой	ACE	2024-10-17	✓
9	Критическая	CVE-2024-4577	cPanel EasyApache	Сетевой	ACE	2024-10-17	✓
10	Критическая	CVE-2024-9047	WordPress File Upload plugin	Сетевой	OAF	2024-10-17	✓
11	Высокая	CVE-2024-7994	Autodesk Revit	Локальный	ACE	2024-10-17	✓
12	Высокая	CVE-2024-7993	Autodesk Revit	Локальный	ACE	2024-10-17	✓
13	Высокая	CVE-2024-20458	Cisco ATA 190 Series Analog Telephone Adapter Firmware	Сетевой	SB	2024-10-17	✓

14	Высокая	CVE-2024-47963	Delta Electronics CNCSoft-G2	Локальный	ACE	2024-10-16	✓
15	Высокая	CVE-2024-47965	Delta Electronics CNCSoft-G2	Локальный	OSI	2024-10-16	✓
16	Высокая	CVE-2024-47964	Delta Electronics CNCSoft-G2	Локальный	ACE	2024-10-16	✓
17	Высокая	CVE-2024-47966	Delta Electronics CNCSoft-G2	Локальный	ACE	2024-10-16	✓
18	Высокая	CVE-2024-47962	Delta Electronics CNCSoft-G2	Локальный	ACE	2024-10-16	✓
19	Высокая	CVE-2024-9122	Google ChromeOS	Сетевой	ACE	2024-10-16	✓
20	Высокая	CVE-2024-9123	Google ChromeOS	Сетевой	ACE	2024-10-16	✓
21	Критическая	CVE-2024-23807	Oracle Communications Messaging Server, Network Charging and Control и Convergent Charging Controller	Сетевой	ACE	2024-10-15	✓
22	Критическая	CVE-2024-29133	Oracle Communications Order and Service Management	Сетевой	ACE	2024-10-15	✓
23	Критическая	CVE-2024-4577	Oracle SD-WAN Aware	Сетевой	ACE	2024-10-15	✓
24	Критическая	CVE-2024-37371	Oracle Communications Cloud Native Core Security Edge Protection Proxy и Cloud Native Core Policy	Сетевой	OSI	2024-10-15	✓
25	Высокая	CVE-2023-46136	Oracle Communications Cloud Native Core Security Edge Protection Proxy	Смежная сеть	DoS	2024-10-15	✓
26	Высокая	CVE-2023-2953	Oracle Communications Cloud Native Core Security Edge Protection Proxy	Сетевой	DoS	2024-10-15	✓

27	Высокая	CVE-2024-40898	Oracle Communications Cloud Native Core Automated Test Suite	Сетевой	CSRF	2024-10-15	✓
28	Высокая	CVE-2023-46136	Oracle Communications Cloud Native Core Automated Test Suite	Смежная сеть	DoS	2024-10-15	✓
29	Высокая	CVE-2024-43044	Oracle Communications Cloud Native Core Network Slice Selection Function, Cloud Native Core Automated Test Suite, Cloud Native Core Security Edge Protection Proxy и Native Core Policy	Сетевой	ACE	2024-10-15	✓
30	Высокая	CVE-2024-33602	Oracle Communications Session Border Controller	Сетевой	DoS	2024-10-15	✓
31	Высокая	CVE-2024-6387	Oracle Communications Session Border Controller	Сетевой	ACE	2024-10-15	✓
32	Высокая	CVE-2024-0450	Oracle Communications Session Border Controller	Сетевой	DoS	2024-10-15	✓
33	Высокая	CVE-2024-34750	Oracle Communications User Data Repository	Сетевой	DoS	2024-10-15	✓
34	Критическая	CVE-2024-25062	Oracle Communications User Data Repository	Сетевой	ACE	2024-10-15	✓
35	Высокая	CVE-2024-9743	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
36	Высокая	CVE-2024-9748	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
37	Высокая	CVE-2024-9738	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
38	Высокая	CVE-2024-9742	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓

39	Высокая	CVE-2024-9740	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
40	Высокая	CVE-2024-9747	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
41	Высокая	CVE-2024-9746	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
42	Высокая	CVE-2024-9741	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
43	Высокая	CVE-2024-9745	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
44	Высокая	CVE-2024-9750	Kofax Power PDF	Сетевой	OSI	2024-10-14	✓
45	Высокая	CVE-2024-9739	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
46	Высокая	CVE-2024-9737	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
47	Высокая	CVE-2024-9736	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
48	Высокая	CVE-2024-9733	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
49	Высокая	CVE-2024-9734	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
50	Высокая	CVE-2024-9764	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
51	Высокая	CVE-2024-9732	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
52	Высокая	CVE-2024-9735	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
53	Высокая	CVE-2024-9755	Kofax Power PDF	Сетевой	OSI	2024-10-14	✓

54	Высокая	CVE-2024-9744	Kofax Power PDF	Сетевой	ACE	2024-10-14	✓
55	Высокая	CVE-2024-45148	Adobe Commerce and Magento Open Source	Сетевой	SB	2024-10-14	✓
56	Высокая	CVE-2024-45116	Adobe Commerce and Magento Open Source	Сетевой	XSS\CSS	2024-10-14	✓
57	Высокая	CVE-2024-45117	Adobe Commerce and Magento Open Source	Сетевой	OSI	2024-10-14	✓
58	Критическая	CVE-2024-45115	Adobe Commerce and Magento Open Source	Сетевой	SB	2024-10-14	✓
59	Высокая	CVE-2024-20501	Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices	Сетевой	DoS	2024-10-04	✓
60	Высокая	CVE-2024-20499	Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices	Сетевой	DoS	2024-10-04	✓
61	Высокая	CVE-2024-20498	Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices	Сетевой	DoS	2024-10-04	✓
62	Критическая	CVE-2024-20521	Cisco Small Business RV042, RV042G, RV320 and RV325 Routers	Сетевой	ACE	2024-10-03	✗
63	Критическая	CVE-2024-20520	Cisco Small Business RV042, RV042G, RV320 and RV325 Routers	Сетевой	ACE	2024-10-03	✗
64	Критическая	CVE-2024-20519	Cisco Small Business RV042, RV042G, RV320 and RV325 Routers	Сетевой	ACE	2024-10-03	✗
65	Критическая	CVE-2024-20518	Cisco Small Business RV042, RV042G, RV320 and RV325 Routers	Сетевой	ACE	2024-10-03	✗

66	Высокая	CVE-2024-47499	Junos OS and Junos OS Evolved RPD	Сетевой	DoS	2024-10-10	✓
67	Высокая	CVE-2024-47502	Junos OS Evolved	Сетевой	DoS	2024-10-10	✓
68	Высокая	CVE-2024-47497	Junos OS httpd	Сетевой	DoS	2024-10-11	✓
69	Высокая	CVE-2024-39525	Junos OS and Junos OS Evolved rpd	Сетевой	ACE	2024-10-11	✓

Краткое описание: Выполнение произвольного кода в Trend Micro Cloud Edge REST API

Идентификатор уязвимости: CVE-2024-48904

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

Уязвимый продукт: Cloud Edge: до 7.0 1081

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

1 **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: 2024-10-18 / 2024-10-18

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1418/>
- <http://success.trendmicro.com/en-US/solution/KA-0017998>

Краткое описание: Отказ в обслуживании в cPanel EasyApache

Идентификатор уязвимости: CVE-2024-36387
BDU:2024-05194

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: EasyApache: 4 - 4 20201-3-3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

2

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: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://news.cpanel.com/easyapache4-2024-07-10-maintenance-and-security-release/>
- <https://bdu.fstec.ru/vul/2024-05194>

Краткое описание: Получение конфиденциальной информации в cPanel EasyApache

Идентификатор уязвимости: CVE-2024-36138
BDU:2024-05133

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

Уязвимый продукт: EasyApache: 4 - 4 20201-3-3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

3

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://news.cpanel.com/easyapache4-2024-07-10-maintenance-and-security-release/>
- <https://bdu.fstec.ru/vul/2024-05133>

Краткое описание: Выполнение произвольного кода в cPanel EasyApache

Идентификатор уязвимости: CVE-2024-38475
BDU:2024-04936

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: EasyApache: 4 - 4 20201-3-3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://news.cpanel.com/easyapache4-2024-07-10-maintenance-and-security-release/>
- <https://bdu.fstec.ru/vul/2024-04936>

Краткое описание: Подделка запросов на стороне сервера в cPanel EasyApache

Идентификатор уязвимости: CVE-2024-38476
BDU:2024-05131

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

Уязвимый продукт: EasyApache: 4 - 4 20201-3-3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Подделка запросов на стороне сервера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://news.cpanel.com/easyapache4-2024-07-10-maintenance-and-security-release/>
- <https://bdu.fstec.ru/vul/2024-05131>

Краткое описание: Отказ в обслуживании в cPanel EasyApache

Идентификатор уязвимости: CVE-2024-38477
BDU:2024-05195

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: EasyApache: 4 - 4 20201-3-3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Отказ в обслуживании

- 6 **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: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://news.cpanel.com/easyapache4-2024-07-10-maintenance-and-security-release/>
- <https://bdu.fstec.ru/vul/2024-05195>

Краткое описание: Обход безопасности в cPanel EasyApache

Идентификатор уязвимости: CVE-2024-8927
BDU:2024-07679

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: EasyApache: 4 - 4 20201-3-3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

- 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: 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: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://news.cpanel.com/easyapache4-2024-10-02-maintenance-and-security-release/>
- <https://bdu.fstec.ru/vul/2024-07679>

Краткое описание: Выполнение произвольного кода в cPanel EasyApache

Идентификатор уязвимости: CVE-2024-8926
BDU:2024-07677

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

Уязвимый продукт: EasyApache: 4 - 4 20201-3-3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://news.cpanel.com/easyapache4-2024-10-02-maintenance-and-security-release/>
- <https://bdu.fstec.ru/vul/2024-07677>

Краткое описание: Выполнение произвольного кода в cPanel EasyApache

Идентификатор уязвимости: CVE-2024-4577
BDU:2024-04432

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

Уязвимый продукт: EasyApache: 4 - 4 20201-3-3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://news.cpanel.com/easyapache4-2024-10-02-maintenance-and-security-release/>
- <https://bdu.fstec.ru/vul/2024-04432>

Краткое описание: Перезапись произвольных файлов в WordPress File Upload plugin

Идентификатор уязвимости: CVE-2024-9047

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

Уязвимый продукт: WordPress File Upload: 4.24.0 - 4.24.11

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Перезапись произвольных файлов

10

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:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://www.wordfence.com/threat-intel/vulnerabilities/id/554a314c-9e8e-4691-9792-d086790ef40f?source=cve>
- <http://plugins.trac.wordpress.org/changeset/3164449/wp-file-upload>

Краткое описание: Выполнение произвольного кода в Autodesk Revit

Идентификатор уязвимости: CVE-2024-7994

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Revit: 2024 - 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0017>

Краткое описание: Выполнение произвольного кода в Autodesk Revit

Идентификатор уязвимости: CVE-2024-7993

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Revit: 2024 - 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0018>

Краткое описание: Обход безопасности в Cisco ATA 190 Series Analog Telephone Adapter Firmware

Идентификатор уязвимости: CVE-2024-20458

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: ATA 191 Multiplatform Analog Telephone Adapter : 11.2.4 - 12.0.1
ATA 192 Multiplatform Analog Telephone Adapter : 11.2.4
ATA 190 Series Analog Telephone Adapters: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-17 / 2024-10-17

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multi-RDTEqRsy>

Краткое описание: Выполнение произвольного кода в Delta Electronics CNCSoft-G2

Идентификатор уязвимости: CVE-2024-47963

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: CNCSoft-G2: 2.1.0.10

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Локальный

14 **Взаимодействие с пользователем:** Требуется

Дата выявления / Дата обновления: 2024-10-16 / 2024-10-16

Ссылки на источник:

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-284-21>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1384/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1386/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1387/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1385/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1391/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1392/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1393/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1394/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1400/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1403/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1408/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1409/>

Краткое описание: Получение конфиденциальной информации в Delta Electronics CNCSoft-G2

Идентификатор уязвимости: CVE-2024-47965

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: CNCSoft-G2: 2.1.0.10

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-16 / 2024-10-16

Ссылки на источник:

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-284-21>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1388/>

Краткое описание: Выполнение произвольного кода в Delta Electronics CNCSoft-G2

Идентификатор уязвимости: CVE-2024-47964

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

Уязвимый продукт: CNCSoft-G2: 2.1.0.10

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-16 / 2024-10-16

Ссылки на источник:

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-284-21>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1399/>

Краткое описание: Выполнение произвольного кода в Delta Electronics CNCSoft-G2

Идентификатор уязвимости: CVE-2024-47966

Идентификатор программной ошибки: CWE-457 Использование неинициализированной переменной

Уязвимый продукт: CNCSoft-G2: 2.1.0.10

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-16 / 2024-10-16

Ссылки на источник:

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-284-21>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1411/>

Краткое описание: Выполнение произвольного кода в Delta Electronics CNCSoft-G2

Идентификатор уязвимости: CVE-2024-47962

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: CNCSoft-G2: 2.1.0.10

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-16 / 2024-10-16

Ссылки на источник:

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-284-21>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1397/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1389/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1390/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1404/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1395/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1396/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1398/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1401/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1402/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1406/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1405/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1407/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1410/>

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-9122
BDU:2024-07574

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

Уязвимый продукт: Chrome OS: до 126.0.6478.255

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

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

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: 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: 2024-10-16 / 2024-10-16

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/10/long-term-support-channel-update-for.html>
- <https://bdu.fstec.ru/vul/2024-07574>

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-9123
BDU:2024-07576

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

Уязвимый продукт: Chrome OS: до 126.0.6478.255

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:N/AC:L/PR:L/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: 2024-10-16 / 2024-10-16

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/10/long-term-support-channel-update-for.html>
- <https://bdu.fstec.ru/vul/2024-07576>

Краткое описание: Выполнение произвольного кода в Oracle Communications Messaging Server, Network Charging and Control и Convergent Charging Controller

Идентификатор уязвимости: CVE-2024-23807
BDU:2024-01559

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Oracle Communications Messaging Server: 8.1
Oracle Communications Network Charging and Control: 6.0.1.0.0 - 15.0.0.0.0
Oracle Communications Convergent Charging Controller: 6.0.1.0.0 - 15.0.0.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?534794>
- <http://www.oracle.com/security-alerts/cpuoct2024.html?936685>
- <http://www.oracle.com/security-alerts/cpuoct2024.html?3209>
- <https://bdu.fstec.ru/vul/2024-01559>

Краткое описание: Выполнение произвольного кода в Oracle Communications Order and Service Management

Идентификатор уязвимости: CVE-2024-29133
BDU:2024-02392

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Oracle Communications Order and Service Management: 7.4.0 - 7.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

22

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

Оценка CVSSv3: 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: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?62362>
- <https://bdu.fstec.ru/vul/2024-02392>

Краткое описание: Выполнение произвольного кода в Oracle SD-WAN Aware

Идентификатор уязвимости: CVE-2024-4577
BDU:2024-04432

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

Уязвимый продукт: Oracle SD-WAN Aware: 9.0.1.10.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

23 **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:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?904642>
- <https://bdu.fstec.ru/vul/2024-04432>

Краткое описание: Получение конфиденциальной информации в Oracle Communications Cloud Native Core Security Edge Protection Proxy и Cloud Native Core Policy

Идентификатор уязвимости: CVE-2024-37371
BDU:2024-07005

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Oracle Communications Cloud Native Core Security Edge Protection Proxy: 23.4.2 - 24.2.0
Oracle Communications Cloud Native Core Policy: 23.4.0 - 23.4.6

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 9.1 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: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?936686>
- <http://www.oracle.com/security-alerts/cpuoct2024.html?936689>
- <https://bdu.fstec.ru/vul/2024-07005>

Краткое описание: Отказ в обслуживании в Oracle Communications Cloud Native Core Security Edge Protection Proxy

Идентификатор уязвимости: CVE-2023-46136

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Oracle Communications Cloud Native Core Security Edge Protection Proxy: 23.4.2 - 24.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?936686>

Краткое описание: Отказ в обслуживании в Oracle Communications Cloud Native Core Security Edge Protection Proxy

Идентификатор уязвимости: CVE-2023-2953
BDU:2023-04057

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Oracle Communications Cloud Native Core Security Edge Protection Proxy: 23.4.2 - 24.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

26 **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: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?936686>
- <https://bdu.fstec.ru/vul/2023-04057>

Краткое описание: Подделка запросов на стороне сервера в Oracle Communications Cloud Native Core Automated Test Suite

Идентификатор уязвимости: CVE-2024-40898
BDU:2024-05368

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

Уязвимый продукт: Oracle Communications Cloud Native Core Automated Test Suite: 23.4.4 - 24.2.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Подделка запросов на стороне сервера

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?947628>
- <https://bdu.fstec.ru/vul/2024-05368>

Краткое описание: Отказ в обслуживании в Oracle Communications Cloud Native Core Automated Test Suite

Идентификатор уязвимости: CVE-2023-46136

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Oracle Communications Cloud Native Core Automated Test Suite: 23.4.3 - 24.2.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?947628>

Краткое описание: Выполнение произвольного кода в Oracle Communications Cloud Native Core Network Slice Selection Function, Cloud Native Core Automated Test Suite, Cloud Native Core Security Edge Protection Proxy и Native Core Policy

Идентификатор уязвимости: CVE-2024-43044
BDU:2024-06145

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Oracle Communications Cloud Native Core Network Slice Selection Function: 24.2.0
Oracle Communications Cloud Native Core Automated Test Suite: 23.4.3 - 24.2.2
Oracle Communications Cloud Native Core Security Edge Protection Proxy: 23.4.2 - 24.2.0
Oracle Communications Cloud Native Core Policy: 23.4.0 - 23.4.6

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

29 **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: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?936692>
- <http://www.oracle.com/security-alerts/cpuoct2024.html?936689>
- <https://bdu.fstec.ru/vul/2024-06145>

Краткое описание: Отказ в обслуживании в Oracle Communications Session Border Controller

Идентификатор уязвимости: CVE-2024-33602
BDU:2024-03601

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

Уязвимый продукт: Oracle Communications Session Border Controller: 9.1.0 - 9.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

30

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?3290>
- <https://bdu.fstec.ru/vul/2024-03601>

Краткое описание: Выполнение произвольного кода в Oracle Communications Session Border Controller

Идентификатор уязвимости: CVE-2024-6387
BDU:2024-04914

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

Уязвимый продукт: Oracle Communications Session Border Controller: 9.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?3290>
- <https://bdu.fstec.ru/vul/2024-04914>

Краткое описание: Отказ в обслуживании в Oracle Communications Session Border Controller

Идентификатор уязвимости: CVE-2024-0450
BDU:2024-04927

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

Уязвимый продукт: Oracle Communications Session Border Controller: 9.2.0 - 9.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

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: 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: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?3290>
- <https://bdu.fstec.ru/vul/2024-04927>

Краткое описание: Отказ в обслуживании в Oracle Communications User Data Repository

Идентификатор уязвимости: CVE-2024-34750
BDU:2024-06407

Идентификатор программной ошибки: CWE-399 Уязвимости, связанные с управлением ресурсами

Уязвимый продукт: Oracle Communications User Data Repository: 12.11.0 - 14.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Отказ в обслуживании

33

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

Оценка CVSSv3: 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: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?3289>
- <https://bdu.fstec.ru/vul/2024-06407>

Краткое описание: Выполнение произвольного кода в Oracle Communications User Data Repository

Идентификатор уязвимости: CVE-2024-25062
BDU:2024-01415

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Oracle Communications User Data Repository: 14.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

34

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

Оценка CVSSv3: 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: 2024-10-15 / 2024-10-15

Ссылки на источник:

- <http://www.oracle.com/security-alerts/cpuoct2024.html?3289>
- <https://bdu.fstec.ru/vul/2024-01415>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9743

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

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1338/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9748

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1339/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9738

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

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

37 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1341/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9742

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

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

38 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1342/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9740

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

39 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1343/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9747

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

40 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1344/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9746

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

41

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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1345/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9741

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

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

42 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1346/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9745

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

43

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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1347/>

Краткое описание: Получение конфиденциальной информации в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9750

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

44 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1348/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9739

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

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

45 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1349/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9737

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

46 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1350/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9736

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

47 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1351/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9733

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

48 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1352/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9734

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

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

49 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1353/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9764

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

50 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1362/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9732

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Power PDF: до 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

51

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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1337/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9735

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF: до 5.1.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

52 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1365/>

Краткое описание: Получение конфиденциальной информации в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9755

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Power PDF: до 5.1.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

53

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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1368/>

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2024-9744

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF: до 5.1.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

54 **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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1364/>

Краткое описание: Обход безопасности в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-45148
BDU:2024-08204

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Adobe Commerce B2B: 1.3.2 - 1.4.2-p2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

55

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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://helpx.adobe.com/security/products/magento/apsb24-73.html>
- <https://bdu.fstec.ru/vul/2024-08204>

Краткое описание: Межсайтовый скриптинг в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-45116

BDU:2024-08202

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

Уязвимый продукт: Adobe Commerce B2B: 1.3.2 - 1.4.2-p2

Magento Open Source: 2.4.0 - 2.4.7-p2

Adobe Commerce (formerly Magento Commerce): 2.4.0 - 2.4.7-p2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

56

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://helpx.adobe.com/security/products/magento/apsb24-73.html>
- <https://bdu.fstec.ru/vul/2024-08202>

Краткое описание: Получение конфиденциальной информации в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-45117
BDU:2024-08215

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Adobe Commerce B2B: 1.3.2 - 1.4.2-p2
Magento Open Source: 2.4.0 - 2.4.7-p2
Adobe Commerce (formerly Magento Commerce): 2.4.0 - 2.4.7-p2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Получение конфиденциальной информации

57

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://helpx.adobe.com/security/products/magento/apsb24-73.html>
- <https://bdu.fstec.ru/vul/2024-08215>

Краткое описание: Обход безопасности в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-45115
BDU:2024-08203

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Adobe Commerce B2B: 1.3.2 - 1.4.2-p2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

58

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: 2024-10-14 / 2024-10-14

Ссылки на источник:

- <http://helpx.adobe.com/security/products/magento/apsb24-73.html>
- <https://bdu.fstec.ru/vul/2024-08203>

Краткое описание: Отказ в обслуживании в Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices

Идентификатор уязвимости: CVE-2024-20501

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Meraki MX: с версии 16.2 по 18.0
Cisco Meraki MX64: все версии
Cisco Meraki MX64W: все версии
Cisco Meraki MX65: все версии
Cisco Meraki MX65W: все версии
Cisco Meraki MX67: все версии
Cisco Meraki MX67C: все версии
Cisco Meraki MX67W: все версии
Cisco Meraki MX68: все версии
Cisco Meraki MX68CW: все версии
Cisco Meraki MX68W: все версии
Cisco Meraki MX75: все версии
Cisco Meraki MX84: все версии
Cisco Meraki MX85: все версии
Cisco Meraki MX95: все версии
Cisco Meraki MX100: все версии
Cisco Meraki MX105: все версии
Cisco Meraki MX250: все версии
Cisco Meraki MX400: все версии
Cisco Meraki MX450: все версии
Cisco Meraki MX600: все версии
Cisco Meraki vMX: все версии
Cisco Meraki Z3: все версии
Cisco Meraki Z3Z3C: все версии
Cisco Meraki Z3Z4: все версии
Cisco Meraki Z3Z4C: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2024-10-04 / 2024-10-04

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2>

Краткое описание: Отказ в обслуживании в Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices

Идентификатор уязвимости: CVE-2024-20499
BDU:2024-07994

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Meraki MX: 16.2 - 18.0
Cisco Meraki MX64: все версии
Cisco Meraki MX64W: все версии
Cisco Meraki MX65: все версии
Cisco Meraki MX65W: все версии
Cisco Meraki MX67: все версии
Cisco Meraki MX67C: все версии
Cisco Meraki MX67W: все версии
Cisco Meraki MX68: все версии
Cisco Meraki MX68CW: все версии
Cisco Meraki MX68W: все версии
Cisco Meraki MX75: все версии
Cisco Meraki MX84: все версии
Cisco Meraki MX85: все версии
Cisco Meraki MX95: все версии
Cisco Meraki MX100: все версии
Cisco Meraki MX105: все версии
Cisco Meraki MX250: все версии
Cisco Meraki MX400: все версии
Cisco Meraki MX450: все версии
Cisco Meraki MX600: все версии
Cisco Meraki vMX: все версии
Cisco Meraki Z3: все версии
Cisco Meraki Z3Z3C: все версии
Cisco Meraki Z3Z4: все версии
Cisco Meraki Z3Z4C: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2024-10-04 / 2024-10-04

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2>
- <https://bdu.fstec.ru/vul/2024-07994>

Краткое описание: Отказ в обслуживании в Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices

Идентификатор уязвимости: CVE-2024-20498

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Meraki MX: 16.2 - 18.0

Cisco Meraki MX64: все версии
Cisco Meraki MX64W: все версии
Cisco Meraki MX65: все версии
Cisco Meraki MX65W: все версии
Cisco Meraki MX67: все версии
Cisco Meraki MX67C: все версии
Cisco Meraki MX67W: все версии
Cisco Meraki MX68: все версии
Cisco Meraki MX68CW: все версии
Cisco Meraki MX68W: все версии
Cisco Meraki MX75: все версии
Cisco Meraki MX84: все версии
Cisco Meraki MX85: все версии
Cisco Meraki MX95: все версии
Cisco Meraki MX100: все версии
Cisco Meraki MX105: все версии
Cisco Meraki MX250: все версии
Cisco Meraki MX400: все версии
Cisco Meraki MX450: все версии
Cisco Meraki MX600: все версии
Cisco Meraki vMX: все версии
Cisco Meraki Z3: все версии
Cisco Meraki Z3Z3C: все версии
Cisco Meraki Z3Z4: все версии
Cisco Meraki Z3Z4C: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2024-10-04 / 2024-10-04

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2>

Краткое описание: Выполнение произвольного кода в Cisco Small Business RV042, RV042G, RV320 and RV325 Routers

Идентификатор уязвимости: CVE-2024-20521

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

Уязвимый продукт: Cisco RV042 Dual WAN VPN Router: все версии
Cisco RV042G Dual Gigabit WAN VPN Router: все версии
RV320 Dual Gigabit WAN VPN Router : все версии
RV325 Dual Gigabit WAN VPN Router : все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

62

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-03 / 2024-10-03

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yj2OSDhV

Краткое описание: Выполнение произвольного кода в Cisco Small Business RV042, RV042G, RV320 and RV325 Routers

Идентификатор уязвимости: CVE-2024-20520

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

Уязвимый продукт: Cisco RV042 Dual WAN VPN Router: все версии
Cisco RV042G Dual Gigabit WAN VPN Router: все версии
RV320 Dual Gigabit WAN VPN Router : все версии
RV325 Dual Gigabit WAN VPN Router : все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

63

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-03 / 2024-10-03

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yj2OSDhV

Краткое описание: Выполнение произвольного кода в Cisco Small Business RV042, RV042G, RV320 and RV325 Routers

Идентификатор уязвимости: CVE-2024-20519

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

Уязвимый продукт: Cisco RV042 Dual WAN VPN Router: все версии
Cisco RV042G Dual Gigabit WAN VPN Router: все версии
RV320 Dual Gigabit WAN VPN Router : все версии
RV325 Dual Gigabit WAN VPN Router : все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

64

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-03 / 2024-10-03

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yj2OSDhV

Краткое описание: Выполнение произвольного кода в Cisco Small Business RV042, RV042G, RV320 and RV325 Routers

Идентификатор уязвимости: CVE-2024-20518

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

Уязвимый продукт: Cisco RV042 Dual WAN VPN Router: все версии
Cisco RV042G Dual Gigabit WAN VPN Router: все версии
RV320 Dual Gigabit WAN VPN Router : все версии
RV325 Dual Gigabit WAN VPN Router : все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

65

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-03 / 2024-10-03

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yj2OSDhV

Краткое описание: Отказ в обслуживании в Junos OS and Junos OS Evolved RPD

Идентификатор уязвимости: CVE-2024-47499

Идентификатор программной ошибки: CWE-754 Некорректная проверка наличия нестандартных условий или исключений

Уязвимый продукт: Juniper Junos OS: с версии 21.2R1 по 23.4R2-S3
Junos OS Evolved: с версии 21.2-EVO по 23.2R2-EVO

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

66 **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: 2024-10-10 / 2024-10-10

Ссылки на источник:

- <http://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-BMP-scenario-receipt-of-a-malformed-AS-PATH-attribute-can-cause-an-RPD-core-CVE-2024-47499>

Краткое описание: Отказ в обслуживании в Junos OS Evolved

Идентификатор уязвимости: CVE-2024-47502

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Junos OS Evolved: с версии 21.4R1-EVO по 23.2R2-EVO

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

67

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: 2024-10-10 / 2024-10-10

Ссылки на источник:

- <http://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-JunOS-Evolved-TCP-session-state-is-not-always-cleared-on-the-Routing-Engine-CVE-2024-47502>

Краткое описание: Отказ в обслуживании в Junos OS httpd

Идентификатор уязвимости: CVE-2024-47497

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

Уязвимый продукт: Juniper Junos OS: с версии 21.4R1 по 24.2R1-S1

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

68

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: 2024-10-11 / 2024-10-11

Ссылки на источник:

- <http://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-JunOS-SRX-Series-QFX-Series-MX-Series-and-EX-Series-Receiving-specific-HTTPS-traffic-causes-resource-exhaustion-CVE-2024-47497>

Краткое описание: Выполнение произвольного кода в Junos OS and Junos OS Evolved rpd

Идентификатор уязвимости: CVE-2024-39525

Идентификатор программной ошибки: CWE-703 Некорректная проверка или обработка исключительных ситуаций

Уязвимый продукт: Junos OS Evolved: 21.2-EVO - 23.2R2-EVO
Juniper Junos OS: 21.2R1 - 24.2R1-S1

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

Способ эксплуатации: Отправки специально сформированного eBGP-трафика

Последствия эксплуатации: Выполнение произвольного кода

69 **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: 2024-10-11 / 2024-10-11

Ссылки на источник:

- <http://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-When-BGP-next-hop-trace-options-is-enabled-receipt-of-specially-crafted-BGP-packet-causes-RPD-crash-CVE-2024-39525>