НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-09-23.1 | 23 сентября 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-40766	SonicWall SonicOS	Сетевой	DoS	2024-08-22	✓
2	Высокая	CVE-2024-20398	Cisco IOS XR CLI	Локальный	PE	2024-09-12	✓
3	Высокая	CVE-2024-45862	Kastle Systems Access Control System	Сетевой	OSI	2024-09-23	✓
4	Высокая	CVE-2024-45861	Kastle Systems Access Control System	Сетевой	OSI	2024-09-23	✓
5	Критическая	CVE-2024-45229	Versa Director	Сетевой	OSI	2024-09-23	✓
6	Высокая	CVE-2024-38475	F5 BIG-IP Apache HTTPD component и Traffix SDC	Сетевой	ACE	2024-09-23	✗
7	Критическая	CVE-2024-38474	F5 BIG-IP Apache HTTPD component и Traffix SDC	Сетевой	ACE	2024-09-23	✗
8	Высокая	CVE-2024-43496	Microsoft Edge	Сетевой	ACE	2024-09-20	✓
9	Высокая	CVE-2024-43489	Microsoft Edge	Сетевой	ACE	2024-09-20	✓
10	Критическая	CVE-2024-8963	Ivanti Cloud Service Appliance	Сетевой	RLF	2024-09-19	✓
11	Высокая	CVE-2024-38016	Microsoft Office Visio	Локальный	ACE	2024-09-19	✓
12	Высокая	CVE-2024-8847	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	OSI	2024-09-19	✓

13	Высокая	CVE-2024-8842	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	ACE	2024-09-19	✓
14	Высокая	CVE-2024-8813	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	ACE	2024-09-19	✓
15	Высокая	CVE-2024-8814	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	OSI	2024-09-19	✓
16	Высокая	CVE-2024-8815	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	ACE	2024-09-19	✓
17	Высокая	CVE-2024-8817	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	ACE	2024-09-19	✓
18	Высокая	CVE-2024-8818	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	ACE	2024-09-19	✓
19	Высокая	CVE-2024-8825	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	OSI	2024-09-19	✓
20	Высокая	CVE-2024-8826	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	OSI	2024-09-19	✓
21	Высокая	CVE-2024-8827	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	ACE	2024-09-19	✓
22	Высокая	CVE-2024-8830	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	ACE	2024-09-19	✓
23	Высокая	CVE-2024-8831	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	OSI	2024-09-19	✓
24	Высокая	CVE-2024-8833	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	OSI	2024-09-19	✓

25	Высокая	CVE-2024-8837	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	OSI	2024-09-19	✓
26	Высокая	CVE-2024-8838	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	OSI	2024-09-19	✓
27	Высокая	CVE-2024-8840	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	OSI	2024-09-19	✓
28	Высокая	CVE-2024-8812	PDF-XChange Editor, PDF-Tools and PDF-XChange PRO	Сетевой	OSI	2024-09-19	✓
29	Критическая	CVE-2024-8807	Cohesive Networks VNS3	Сетевой	ACE	2024-09-18	✓
30	Высокая	CVE-2024-8808	Cohesive Networks VNS3	Сетевой	ACE	2024-09-18	✓
31	Высокая	CVE-2024-8809	Cohesive Networks VNS3	Сетевой	ACE	2024-09-18	✓
32	Критическая	CVE-2024-8806	Cohesive Networks VNS3	Сетевой	ACE	2024-09-18	✓
33	Критическая	CVE-2024-45409	SAML-Toolkits ruby-saml	Сетевой	SB	2024-09-18	✓
34	Высокая	CVE-2024-8907	Google Chrome и Microsoft Edge	Сетевой	OSI	2024-09-18	✓
35	Высокая	CVE-2024-8904	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-09-18	✓
36	Высокая	CVE-2024-38813	VMware vCenter Server	Сетевой	PE	2024-09-17	✓
37	Критическая	CVE-2024-38812	VMware vCenter Server	Сетевой	ACE	2024-09-17	✓
38	Высокая	CVE-2024-45698	D-Link wireless routers	Сетевой	ACE	2024-09-17	✓

39	Критическая	CVE-2024-45697	D-Link wireless routers	Сетевой	ACE	2024-09-17	✓
40	Высокая	CVE-2024-45696	D-Link wireless routers	Смежная сеть	OSI	2024-09-17	✓
41	Критическая	CVE-2024-45695	D-Link wireless routers	Сетевой	ACE	2024-09-17	✓
42	Критическая	CVE-2024-45694	D-Link wireless routers	Сетевой	ACE	2024-09-17	✓
43	Высокая	CVE-2024-40860	Apple macOS Sonoma и Sequoia	Локальный	PE	2024-09-17	✓
44	Высокая	CVE-2024-27876	Apple macOS Sonoma, Ventura и Sequoia	Сетевой	ACE	2024-09-17	✓
45	Высокая	CVE-2024-20696	Libarchive	Сетевой	ACE	2024-09-16	✓
46	Высокая	CVE-2024-20446	Cisco NX-OS Software	Сетевой	DoS	2024-08-29	✓
47	Высокая	CVE-2024-20375	Cisco Unified Communications Manager	Сетевой	DoS	2024-08-21	✓
48	Высокая	CVE-2024-21757	FortiManager и FortiAnalyzer	Локальный	ACE	2024-08-14	✓

1

Краткое описание: Отказ в обслуживании в SonicWall SonicOS

Идентификатор уязвимости: CVE-2024-40766
BDU:2024-06461

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: SonicOS: до 7.0.1-5035

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: 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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015
- https://bdu.fstec.ru/vul/2024-06461

2

Краткое описание: Повышение привилегий в Cisco IOS XR CLI

Идентификатор уязвимости: CVE-2024-20398

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

Уязвимый продукт: Cisco IOS XR: 7.0 - 24.1.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-12 / 2024-09-12

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-priv-esc-CrG5vhCq
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwj25248

3

Краткое описание: Получение конфиденциальной информации в Kastle Systems Access Control System

Идентификатор уязвимости: CVE-2024-45862

Идентификатор программной ошибки: CWE-312 Хранение важных данных в незашифрованном виде

Уязвимый продукт: Access Control System: все версии

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-23 / 2024-09-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-263-05

4

Краткое описание: Получение конфиденциальной информации в Kastle Systems Access Control System

Идентификатор уязвимости: CVE-2024-45861

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

Уязвимый продукт: Access Control System: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование жестко закодированных учетных данных

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-23 / 2024-09-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-263-05

5

Краткое описание: Получение конфиденциальной информации в Versa Director

Идентификатор уязвимости: CVE-2024-45229

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

Уязвимый продукт: Versa Director: до 22.1.4 HF

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 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: 2024-09-23 / 2024-09-23

Ссылки на источник:

- http://security-portal.versa-networks.com/emailbulletins/66e4a8ebda545d61ec2b1ab9

6

Краткое описание: Выполнение произвольного кода в F5 BIG-IP Apache HTTPD component и Traffix SDC

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

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: BIG-IP: 15.0.0 - 17.1.1.3
Traffix SDC: 5.1.0 - 5.2.5

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: 8.1 AV:N/AC:H/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: 2024-09-23 / 2024-09-23

Ссылки на источник:

- http://my.f5.com/manage/s/article/K000140620
- https://bdu.fstec.ru/vul/2024-04936

7

Краткое описание: Выполнение произвольного кода в F5 BIG-IP Apache HTTPD component и Traffix SDC

Идентификатор уязвимости: CVE-2024-38474
BDU:2024-06593

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: BIG-IP: 15.0.0 - 17.1.1.3
Traffix SDC: 5.1.0 - 5.2.5

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-23 / 2024-09-23

Ссылки на источник:

- http://my.f5.com/manage/s/article/K000140620
- https://bdu.fstec.ru/vul/2024-06593

8

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-43496

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 128.0.2739.79

Категория уязвимого продукта: Операционные системы Microsoft 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: 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: 2024-09-20 / 2024-09-20

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-43496

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-43489

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 128.0.2739.79

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-20 / 2024-09-20

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-43489

10

Краткое описание: Чтение локальных файлов в Ivanti Cloud Service Appliance

Идентификатор уязвимости: CVE-2024-8963

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

Уязвимый продукт: Ivanti Cloud Services Appliance (CSA): до 4.6 Patch 519

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.ivanti.com/blog/cloud-service-appliance-4-6-security-update
- http://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963

11

Краткое описание: Выполнение произвольного кода в Microsoft Office Visio

Идентификатор уязвимости: CVE-2024-38016

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

Уязвимый продукт: Microsoft Office: до 16.0.5465.1001
Microsoft Visio: до 16.0.5465.1001
Microsoft 365 Apps for Enterprise: до 16.0.5465.1001

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38016

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8847

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.4.0.388
PDF-Tools: до 10.4.0.388
PDF-XChange PRO: до 10.4.0.388

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

12

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

Оценка CVSSv3: 8.8 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1270/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8842

Идентификатор программной ошибки: CWE-457 Использование неинициализированной переменной

Уязвимый продукт: PDF-XChange Editor: до 10.4.0.388
PDF-Tools: до 10.4.0.388
PDF-XChange PRO: до 10.4.0.388

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

13 **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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1265/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8813

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1236/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8814

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1237/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8815

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

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1238/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8817

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1240/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8818

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1241/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8825

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1248/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8826

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

20

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

Оценка CVSSv3: 8.8 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1249/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8827

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

21

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

Оценка CVSSv3: 8.8 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1250/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8830

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1253/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8831

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1254/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8833

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1256/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8837

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

25

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

Оценка CVSSv3: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1260/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8838

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1261/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8840

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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: 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1263/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor, PDF-Tools and PDF-XChange PRO

Идентификатор уязвимости: CVE-2024-8812

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.1.387
PDF-Tools: до 10.3.1.387
PDF-XChange PRO: до 10.3.1.387

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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: 8.8 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: 2024-09-19 / 2024-09-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1235/
- http://www.pdf-xchange.com/index.php/support/security-bulletins.html

Краткое описание: Выполнение произвольного кода в Cohesive Networks VNS3

Идентификатор уязвимости: CVE-2024-8807

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

Уязвимый продукт: VNS3: до 6.6.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.8 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: 2024-09-18 / 2024-09-18

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1231/
- http://cohesive.net/support/security-responses/

Краткое описание: Выполнение произвольного кода в Cohesive Networks VNS3

Идентификатор уязвимости: CVE-2024-8808

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

Уязвимый продукт: VNS3: до 6.6.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-18 / 2024-09-18

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1232/
- http://cohesive.net/support/security-responses/

Краткое описание: Выполнение произвольного кода в Cohesive Networks VNS3

Идентификатор уязвимости: CVE-2024-8809

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

Уязвимый продукт: VNS3: до 6.6.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-18 / 2024-09-18

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1233/
- http://cohesive.net/support/security-responses/

Краткое описание: Выполнение произвольного кода в Cohesive Networks VNS3

Идентификатор уязвимости: CVE-2024-8806

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

Уязвимый продукт: VNS3: до 6.6.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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: 9.8 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: 2024-09-18 / 2024-09-18

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1230/
- http://cohesive.net/support/security-responses/

33

Краткое описание: Обход безопасности в SAML-Toolkits ruby-saml

Идентификатор уязвимости: CVE-2024-45409
BDU:2024-07261

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: SAML SSO for Ruby: 1.0.0 - 1.16.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-18 / 2024-09-18

Ссылки на источник:

- http://github.com/SAML-Toolkits/ruby-saml/security/advisories/GHSA-jw9c-mfg7-9rx2
- http://github.com/SAML-Toolkits/ruby-saml/commit/1ec5392bc506fe43a02dbb66b68741051c5ffeae
- http://github.com/SAML-Toolkits/ruby-saml/commit/4865d030cae9705ee5cdb12415c654c634093ae7
- https://bdu.fstec.ru/vul/2024-07261

34

Краткое описание: Получение конфиденциальной информации в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-8907

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.138
Microsoft Edge: 79.0.309.71 - 128.0.2739.79

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2024-09-18 / 2024-09-18

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_17.html
- http://crbug.com/360642942
- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-8907

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-8904

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.138
Microsoft Edge: 79.0.309.71 - 128.0.2739.79

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 2024-09-18 / 2024-09-18

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_17.html
- http://crbug.com/365376497
- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-8904

Краткое описание: Повышение привилегий в VMware vCenter Server

Идентификатор уязвимости: CVE-2024-38813

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: vCenter Server: 7.0 U1 - 8.0.0c

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Повышение привилегий

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-17 / 2024-09-17

Ссылки на источник:

- http://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968

Краткое описание: Выполнение произвольного кода в VMware vCenter Server

Идентификатор уязвимости: CVE-2024-38812
BDU:2024-07209

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

Уязвимый продукт: vCenter Server: 7.0 U1 - 8.0.0c

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 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: 2024-09-17 / 2024-09-17

Ссылки на источник:

- http://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968
- https://bdu.fstec.ru/vul/2024-07209

38

Краткое описание: Выполнение произвольного кода в D-Link wireless routers

Идентификатор уязвимости: CVE-2024-45698

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

Уязвимый продукт: DIR-X4860: 1.04B04_Hot-Fix

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-17 / 2024-09-17

Ссылки на источник:

- http://www.twcert.org.tw/tw/cp-132-8090-bf06b-1.html
- http://www.twcert.org.tw/en/cp-139-8091-bcd52-2.html
- http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412

39

Краткое описание: Выполнение произвольного кода в D-Link wireless routers

Идентификатор уязвимости: CVE-2024-45697

Идентификатор программной ошибки: CWE-912 Скрытые функции

Уязвимый продукт: DIR-X4860: 1.04B04_Hot-Fix

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: 2024-09-17 / 2024-09-17

Ссылки на источник:

- http://www.twcert.org.tw/tw/cp-132-8088-590ed-1.html
- http://www.twcert.org.tw/en/cp-139-8089-32df6-2.html
- http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412

Краткое описание: Получение конфиденциальной информации в D-Link wireless routers

Идентификатор уязвимости: CVE-2024-45696

Идентификатор программной ошибки: CWE-912 Скрытые функции

Уязвимый продукт: DIR-X4860: 1.04B04_Hot-Fix
COVR-X1870: 1.02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Использование жестко закодированных учетных данных

Последствия эксплуатации: Получение конфиденциальной информации

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

40

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-17 / 2024-09-17

Ссылки на источник:

- http://www.twcert.org.tw/tw/cp-132-8086-93ed5-1.html
- http://www.twcert.org.tw/en/cp-139-8087-c3e70-2.html
- http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412

41

Краткое описание: Выполнение произвольного кода в D-Link wireless routers

Идентификатор уязвимости: CVE-2024-45695

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DIR-X4860: 1.04B04_Hot-Fix

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Переполнение буфера.

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: 2024-09-17 / 2024-09-17

Ссылки на источник:

- http://www.twcert.org.tw/tw/cp-132-8082-f1687-1.html
- http://www.twcert.org.tw/en/cp-139-8083-a299e-2.html
- http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412

Краткое описание: Выполнение произвольного кода в D-Link wireless routers

Идентификатор уязвимости: CVE-2024-45694

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DIR-X4860: 1.04B04_Hot-Fix
DIR-X5460: 1.11B01_Hot-Fix

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Переполнение буфера.

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.

42

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: 2024-09-17 / 2024-09-17

Ссылки на источник:

- http://www.twcert.org.tw/tw/cp-132-8080-7f494-1.html
- http://www.twcert.org.tw/en/cp-139-8081-3fb39-2.html
- http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412

Краткое описание: Повышение привилегий в Apple macOS Sonoma и Sequoia

Идентификатор уязвимости: CVE-2024-40860

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: macOS Sonoma: 14.0 23A344 - 14.6.1 23G93
macOS: до 15.0 24A335

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-17 / 2024-09-17

Ссылки на источник:

- http://support.apple.com/en-us/121247
- http://support.apple.com/en-us/121238

Краткое описание: Выполнение произвольного кода в Apple macOS Sonoma, Ventura и Sequoia

Идентификатор уязвимости: CVE-2024-27876

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

Уязвимый продукт: macOS Sonoma: 14.0 23A344 - 14.6.1 23G93
macOS Ventura: 13.0 22A380 - 13.6.9 22G830
macOS Sequoia: до 15.0 24A335

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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: 2024-09-17 / 2024-09-17

Ссылки на источник:

- http://support.apple.com/en-us/121247
- http://support.apple.com/en-us/121234
- http://support.apple.com/en-us/121238

Краткое описание: Выполнение произвольного кода в Libarchive

Идентификатор уязвимости: CVE-2024-20696
BDU:2024-00408

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

Уязвимый продукт: libarchive: 3.0 - 3.7.4

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.

45

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: 2024-09-16 / 2024-09-16

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-20696
- http://github.com/libarchive/libarchive/pull/2172
- http://github.com/libarchive/libarchive/releases/tag/v3.7.5
- https://bdu.fstec.ru/vul/2024-00408

Краткое описание: Отказ в обслуживании в Cisco NX-OS Software

Идентификатор уязвимости: CVE-2024-20446
BDU:2024-06551

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Cisco NX-OS: с версии 8.2(11) по 10.2(1q)
Cisco Nexus 3000 Series Switches: все версии
Cisco Nexus 9000 Series Switches: все версии
Cisco Nexus 9000 Series Switches NX-OS Mode: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

46 **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: 2024-08-29 / 2024-08-29

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dhcp6-relay-dos-znEAA6xn
- https://bdu.fstec.ru/vul/2024-06551

47

Краткое описание: Отказ в обслуживании в Cisco Unified Communications Manager

Идентификатор уязвимости: CVE-2024-20375
BDU:2024-06406

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Cisco Unified Communications Manager: до версии 15SU1

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2024-08-21 / 2024-08-21

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-dos-kkHq43We
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwi68892
- https://bdu.fstec.ru/vul/2024-06406

48

Краткое описание: Выполнение произвольного кода в FortiManager и FortiAnalyzer

Идентификатор уязвимости: CVE-2024-21757

Идентификатор программной ошибки: CWE-620 Смена пароля без подтверждения

Уязвимый продукт: FortiManager и FortiAnalyzer:
FortiManager: 7.0.0 - 7.4.1
FortiAnalyzer: 7.0.0 - 7.4.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://fortiguard.fortinet.com/psirt/FG-IR-23-467