НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-06-17.1 | 17 июня 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-1839	Intrado 911 Emergency Gateway	Сетевой	ACE	2024-06-12	✓
2	Высокая	CVE-2024-28877	MicroDicom DICOM Viewer	Сетевой	ACE	2024-06-12	✓
3	Высокая	CVE-2024-33606	MicroDicom DICOM Viewer	Сетевой	OSI	2024-06-12	✓
4	Высокая	CVE-2024-0985	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	PE	2024-06-13	✓
5	Высокая	CVE-2023-6516	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓
6	Высокая	CVE-2023-3341	Dell SmartFabric OS10	Сетевой	DoS	2024-06-13	✓
7	Высокая	CVE-2023-5679	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓
8	Высокая	CVE-2023-5517	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓
9	Высокая	CVE-2019-19333	Dell SmartFabric OS10	Сетевой	ACE	2024-06-13	✓
10	Высокая	CVE-2023-50868	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓

11	Высокая	CVE-2019-19334	Dell SmartFabric OS10	Сетевой	ACE	2024-06-13	✓
12	Средняя	CVE-2023-50495	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓
13	Высокая	CVE-2019-20393	Dell SmartFabric OS10	Сетевой	ACE	2024-06-13	✓
14	Высокая	CVE-2023-50387	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓
15	Высокая	CVE-2023-4408	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓
16	Высокая	CVE-2023-3341	Dell Enterprise SONiC Distribution	Сетевой	DoS	2024-06-12	✓
17	Высокая	CVE-2024-0553	Dell Enterprise SONiC Distribution	Сетевой	ACE	2024-06-12	✓
18	Высокая	CVE-2023-44487	Dell Enterprise SONiC Distribution	Сетевой	DoS	2024-06-12	✓
19	Высокая	CVE-2023-4692	Dell Enterprise SONiC Distribution	Локальный	ACE	2024-06-12	✓
20	Высокая	CVE-2023-27534	Dell Enterprise SONiC Distribution	Сетевой	ACE	2024-06-12	✓
21	Высокая	CVE-2023-43787	Dell Enterprise SONiC Distribution	Локальный	ACE	2024-06-12	✓
22	Высокая	CVE-2023-0464	Siemens SCALANCE XM-400/XR-500	Сетевой	DoS	2024-06-13	✓
23	Высокая	CVE-2023-0215	Siemens SCALANCE XM-400/XR-500	Сетевой	DoS	2024-06-13	✓

24	Высокая	CVE-2022-4450	Siemens SCALANCE XM-400/XR-500	Сетевой	DoS	2024-06-13	✓
25	Критическая	CVE-2024-30300	Adobe FrameMaker Publishing Server	Сетевой	OSI	2024-06-13	✓
26	Критическая	CVE-2024-30299	Adobe FrameMaker Publishing Server	Сетевой	SB	2024-06-13	✓
27	Высокая	CVE-2021-39537	Dell Enterprise SONiC Distribution	Сетевой	ACE	2024-06-12	✓
28	Высокая	CVE-2023-29491	Dell Enterprise SONiC Distribution	Локальный	ACE	2024-06-12	✓
29	Высокая	CVE-2024-31484	Siemens SICAM AK3 / BC / TM	Локальный	ACE	2024-06-12	✓
30	Высокая	CVE-2024-35303	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-06-12	✓
31	Высокая	CVE-2024-0056	Dell Live Optics Collector	Сетевой	OSI	2024-06-12	✓
32	Высокая	CVE-2024-25062	Dell NetWorker	Сетевой	DoS	2024-06-12	✓
33	Критическая	CVE-2023-41993	Dell NetWorker Runtime Environment (NRE)	Сетевой	ACE	2024-06-12	✓
34	Высокая	CVE-2023-46589	Dell NetWorker	Сетевой	LoI	2024-06-12	✓
35	Высокая	CVE-2024-34115	Adobe Substance 3D Stager	Локальный	ACE	2024-06-12	✓
36	Высокая	CVE-2024-20753	Adobe Photoshop	Локальный	ACE	2024-06-12	✓
37	Высокая	CVE-2024-5513	Kofax Power PDF Advanced	Локальный	ACE	2024-06-05	✓
38	Высокая	CVE-2024-5511	Kofax Power PDF Advanced	Локальный	OSI	2024-06-05	✓

39	Высокая	CVE-2024-5510	Kofax Power PDF Advanced	Локальный	OSI	2024-06-05	✓
40	Высокая	CVE-2024-5306	Kofax Power PDF Advanced	Локальный	ACE	2024-06-05	✓
41	Высокая	CVE-2024-5305	Kofax Power PDF Advanced	Локальный	ACE	2024-06-05	✓
42	Высокая	CVE-2024-5304	Kofax Power PDF Advanced	Локальный	ACE	2024-06-05	✓
43	Высокая	CVE-2024-5303	Kofax Power PDF Advanced	Локальный	ACE	2024-06-05	✓
44	Высокая	CVE-2024-5302	Kofax Power PDF Advanced	Локальный	ACE	2024-06-05	✓
45	Высокая	CVE-2024-5301	Kofax Power PDF Advanced	Локальный	ACE	2024-06-05	✓
46	Высокая	CVE-2024-30373	Kofax Power PDF Advanced	Локальный	ACE	2024-06-05	✓
47	Высокая	CVE-2024-35241	Composer	Сетевой	ACE	2024-06-11	✓
48	Критическая	CVE-2024-28038	Toshiba Tec MFPs	Сетевой	ACE	2024-06-07	✓
49	Высокая	CVE-2024-33605	Toshiba Tec MFPs	Сетевой	RLF	2024-06-07	✓
50	Критическая	CVE-2024-33610	Toshiba Tec MFPs	Сетевой	LoI	2024-06-07	✓
51	Критическая	CVE-2024-35244	Toshiba Tec MFPs	Сетевой	OSI	2024-06-07	✓
52	Критическая	CVE-2024-36248	Toshiba Tec MFPs	Сетевой	OSI	2024-06-07	✓
53	Высокая	CVE-2024-36249	Toshiba Tec MFPs	Сетевой	XSS\CSS	2024-06-07	✓

54	Высокая	CVE-2024-36251	Toshiba Tec MFPs	Сетевой	DoS	2024-06-07	✓
55	Критическая	CVE-2022-30267	Emerson Ovation	Сетевой	ACE	2024-06-07	✓
56	Высокая	CVE-2024-5597	Fuji Electric Monitouch V-SFT	Локальный	ACE	2024-06-05	✓
57	Критическая	CVE-2024-36104	Apache OFBiz	Сетевой	RLF	2024-06-05	✓
58	Критическая	CVE-2024-36081	Westermo EDW-100	Сетевой	OSI	2024-06-06	✗
59	Высокая	CVE-2024-36254	Toshiba Tec MFPs	Сетевой	DoS	2024-06-07	✓
60	Критическая	CVE-2024-32752	Johnson Controls Software House iStar Pro Door Controller and ICU	Сетевой	SB	2024-06-07	✗
61	Высокая	CVE-2024-32004	Git for Windows	Локальный	ACE	2024-06-07	✓
62	Высокая	CVE-2024-34171	Fuji Electric Monitouch V-SFT	Локальный	ACE	2024-06-05	✓
63	Критическая	CVE-2024-36080	Westermo EDW-100	Сетевой	OSI	2024-06-06	✗
64	Критическая	CVE-2022-29966	Emerson Ovation	Сетевой	SB	2024-06-07	✓
65	Критическая	CVE-2024-36522	Apache Wicket	Сетевой	ACE	2024-06-05	✓
66	Критическая	CVE-2024-32002	Git	Сетевой	WLF	2024-06-07	✓
67	Критическая	CVE-2024-32002	Git for Windows	Сетевой	WLF	2024-06-07	✓
68	Высокая	CVE-2024-26256	libarchive	Локальный	ACE	2024-06-05	✓

69	Высокая	CVE-2024-28995	SolarWinds Serv-U	Сетевой	RLF	2024-06-07	✓
70	Высокая	CVE-2024-5271	Fuji Electric Monitouch V-SFT	Локальный	ACE	2024-06-05	✓
71	Высокая	CVE-2024-20360	Cisco Firepower Management Center	Сетевой	ACE	2024-05-22	✓
72	Высокая	CVE-2024-20366	Cisco Crosswork Network Services Orchestrator	Локальный	ACE	2024-05-16	✓
73	Высокая	CVE-2024-31491	FortiSandbox	Сетевой	OAF	2024-05-15	✓

1

Краткое описание: Выполнение произвольного кода в Intrado 911 Emergency Gateway

Идентификатор уязвимости: CVE-2024-1839

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

Уязвимый продукт: 911 Emergency Gateway: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-163-04

2

Краткое описание: Выполнение произвольного кода в MicroDicom DICOM Viewer

Идентификатор уязвимости: CVE-2024-28877

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: MicroDicom DICOM Viewer: до версии 2024.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-163-01

3

Краткое описание: Получение конфиденциальной информации в MicroDicom DICOM Viewer

Идентификатор уязвимости: CVE-2024-33606

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

Уязвимый продукт: MicroDicom DICOM Viewer: до версии 2024.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-163-01

4

Краткое описание: Повышение привилегий в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2024-0985

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Azure Stack: до версии 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная проверка входных 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: 8.0 AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01121

5

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-6516

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

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Переполнение буфера

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities

6

Краткое описание: Отказ в обслуживании в Dell SmartFabric OS10

Идентификатор уязвимости: CVE-2023-3341

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

Уязвимый продукт: SmartFabric OS10: 10.5.5.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224301/dsa-2024-185-security-update-for-dell-os10-third-party-vulnerabilities
- https://bdu.fstec.ru/vul/2023-06079

7

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-5679

Идентификатор программной ошибки: CWE-617 Несанкционированный вызов утверждения

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-04269

8

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-5517

Идентификатор программной ошибки: CWE-617 Несанкционированный вызов утверждения

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-02902

9

Краткое описание: Выполнение произвольного кода в Dell SmartFabric OS10

Идентификатор уязвимости: CVE-2019-19333

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: SmartFabric OS10: 10.5.5.8

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224301/dsa-2024-185-security-update-for-dell-os10-third-party-vulnerabilities
- https://bdu.fstec.ru/vul/2020-02870

10

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-50868

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

Уязвимый продукт: Azure Stack: до версии 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01462

11

Краткое описание: Выполнение произвольного кода в Dell SmartFabric OS10

Идентификатор уязвимости: CVE-2019-19334

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: SmartFabric OS10: 10.5.5.8

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224301/dsa-2024-185-security-update-for-dell-os10-third-party-vulnerabilities

12

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-50495

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 6.5 AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities

Краткое описание: Выполнение произвольного кода в Dell SmartFabric OS10

Идентификатор уязвимости: CVE-2019-20393

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: SmartFabric OS10: 10.5.5.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224301/dsa-2024-185-security-update-for-dell-os10-third-party-vulnerabilities

14

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-50387

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

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01359

15

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-4408

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

Уязвимый продукт: Azure Stack: до версии 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Переполнение буфера

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-02883

16

Краткое описание: Отказ в обслуживании в Dell Enterprise SONiC Distribution

Идентификатор уязвимости: CVE-2023-3341

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

Уязвимый продукт: Enterprise SONiC: до версии 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224731/dsa-2024-191-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
- https://bdu.fstec.ru/vul/2023-06079

17

Краткое описание: Выполнение произвольного кода в Dell Enterprise SONiC Distribution

Идентификатор уязвимости: CVE-2024-0553

Идентификатор программной ошибки: CWE-208 Разглашение информации, связанное с временной разницей при выполнении операций

Уязвимый продукт: Enterprise SONiC: до 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных 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: 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: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224731/dsa-2024-191-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
- https://bdu.fstec.ru/vul/2024-00707

18

Краткое описание: Отказ в обслуживании в Dell Enterprise SONiC Distribution

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: Enterprise SONiC: до 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224731/dsa-2024-191-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
- https://bdu.fstec.ru/vul/2023-06559

19

Краткое описание: Выполнение произвольного кода в Dell Enterprise SONiC Distribution

Идентификатор уязвимости: CVE-2023-4692

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Enterprise SONiC: до 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224731/dsa-2024-191-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
- https://bdu.fstec.ru/vul/2023-06822

20

Краткое описание: Выполнение произвольного кода в Dell Enterprise SONiC Distribution

Идентификатор уязвимости: CVE-2023-27534

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Enterprise SONiC: до 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224731/dsa-2024-191-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
- https://bdu.fstec.ru/vul/2023-02084

21

Краткое описание: Выполнение произвольного кода в Dell Enterprise SONiC Distribution

Идентификатор уязвимости: CVE-2023-43787

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

Уязвимый продукт: Enterprise SONiC: до 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224731/dsa-2024-191-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
- https://bdu.fstec.ru/vul/2023-06816

Краткое описание: Отказ в обслуживании в Siemens SCALANCE XM-400/XR-500

Идентификатор уязвимости: CVE-2023-0464

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

Уязвимый продукт: Siemens SCALANCE XM-400/XR-500:
SCALANCE XR552-12M: до 6.6.1
SCALANCE XR528-6M: до 6.6.1
SCALANCE XR526-8C: до 6.6.1
SCALANCE XR524-8C: до 6.6.1
SCALANCE XM416-4C: до 6.6.1
SCALANCE XM408-8C: до 6.6.1
SCALANCE XM408-4C: до 6.6.1

Категория уязвимого продукта: Телекоммуникационное оборудование

22 **Способ эксплуатации:** Использование специально созданного вредоносного сертификата.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-879734.txt
- https://bdu.fstec.ru/vul/2023-02108

Краткое описание: Отказ в обслуживании в Siemens SCALANCE XM-400/XR-500

Идентификатор уязвимости: CVE-2023-0215

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Siemens SCALANCE XM-400/XR-500:
SCALANCE XR552-12M: до 6.6.1
SCALANCE XR528-6M: до 6.6.1
SCALANCE XR526-8C: до 6.6.1
SCALANCE XR524-8C: до 6.6.1
SCALANCE XM416-4C: до 6.6.1
SCALANCE XM408-8C: до 6.6.1
SCALANCE XM408-4C: до 6.6.1

Категория уязвимого продукта: Телекоммуникационное оборудование

23 **Способ эксплуатации:** Использование памяти после ее освобождения

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-879734.txt
- https://bdu.fstec.ru/vul/2023-00675

Краткое описание: Отказ в обслуживании в Siemens SCALANCE XM-400/XR-500

Идентификатор уязвимости: CVE-2022-4450

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Siemens SCALANCE XM-400/XR-500:
SCALANCE XR552-12M: до 6.6.1
SCALANCE XR528-6M: до 6.6.1
SCALANCE XR526-8C: до 6.6.1
SCALANCE XR524-8C: до 6.6.1
SCALANCE XM416-4C: до 6.6.1
SCALANCE XM408-8C: до 6.6.1
SCALANCE XM408-4C: до 6.6.1

Категория уязвимого продукта: Телекоммуникационное оборудование

24 **Способ эксплуатации:** Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-879734.txt
- https://bdu.fstec.ru/vul/2023-02240

Краткое описание: Получение конфиденциальной информации в Adobe FrameMaker Publishing Server

Идентификатор уязвимости: CVE-2024-30300

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

Уязвимый продукт: Adobe FrameMaker Publishing Server: 2020 Update 3 - 2022.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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: 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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-38.html

Краткое описание: Обход безопасности в Adobe FrameMaker Publishing Server

Идентификатор уязвимости: CVE-2024-30299

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Adobe FrameMaker Publishing Server: 2020 Update 3 - 2022.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-38.html

27

Краткое описание: Выполнение произвольного кода в Dell Enterprise SONiC Distribution

Идентификатор уязвимости: CVE-2021-39537

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Enterprise SONiC: до версии 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224731/dsa-2024-191-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
- https://bdu.fstec.ru/vul/2023-07626

28

Краткое описание: Выполнение произвольного кода в Dell Enterprise SONiC Distribution

Идентификатор уязвимости: CVE-2023-29491

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

Уязвимый продукт: Enterprise SONiC: до версии 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224731/dsa-2024-191-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
- https://bdu.fstec.ru/vul/2023-05772

Краткое описание: Выполнение произвольного кода в Siemens SICAM AK3 / BC / TM

Идентификатор уязвимости: CVE-2024-31484

Идентификатор программной ошибки: CWE-170 Некорректное использование нулевых символов

Уязвимый продукт: CPCX26: до 06.02
ETA4: до 10.46
ETA5: до 03.27
PCCX26: до 06.05

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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: 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: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-871704.html
- http://cert-portal.siemens.com/productcert/html/ssa-620338.html
- https://bdu.fstec.ru/vul/2024-04049

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-35303

Идентификатор программной ошибки: CWE-704 Некорректное преобразование или приведение типов

Уязвимый продукт: Tecnomatix Plant Simulation: до версии 2404.0001

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-900277.html

31

Краткое описание: Получение конфиденциальной информации в Dell Live Optics Collector

Идентификатор уязвимости: CVE-2024-0056

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Live Optics Windows Collector: до версии 25.1.13.152

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000225301/dsa-2024-205-security-update-for-dell-live-optics-collector-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-00281

32

Краткое описание: Отказ в обслуживании в Dell NetWorker

Идентификатор уязвимости: CVE-2024-25062

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: NetWorker: до версии 19.10.0.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000225945/dsa-2024-248-security-update-for-dell-networker-multiple-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01415

33

Краткое описание: Выполнение произвольного кода в Dell NetWorker Runtime Environment (NRE)

Идентификатор уязвимости: CVE-2023-41993

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

Уязвимый продукт: NetWorker Runtime Environment (NRE): версии 8.0.18

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000225215/dsa-2024-224-security-update-for-dell-networker-runtime-environment-nre-vulnerabilities
- https://bdu.fstec.ru/vul/2023-06113

34

Краткое описание: Потеря целостности в Dell NetWorker

Идентификатор уязвимости: CVE-2023-46589

Идентификатор программной ошибки: CWE-444 Некорректная интерпретация HTTP-запросов (несанкционированные HTTP-запросы)

Уязвимый продукт: NetWorker: до версии 19.10.0.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Потеря целостности

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000225945/dsa-2024-248-security-update-for-dell-networker-multiple-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01300

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2024-34115

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: с версии 2.0.0 по 2.1.4

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: 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: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-43.html

Краткое описание: Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости: CVE-2024-20753

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Photoshop: с версии 24.0 по 25.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-06-12 / 2024-06-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/photoshop/apsb24-27.html

37

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-5513

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF Advanced: до версии 5.0.0.21

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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-556/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm

38

Краткое описание: Получение конфиденциальной информации в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-5511

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Power PDF Advanced: до версии 5.0.0.21

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 7.8 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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-554/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm

39

Краткое описание: Получение конфиденциальной информации в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-5510

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Power PDF Advanced: до версии 5.0.0.21

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 7.8 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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-553/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm

40

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-5306

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

Уязвимый продукт: Power PDF Advanced: до 5.0.0.21

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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-551/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm

41

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-5305

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Power PDF Advanced: до версии 5.0.0.21

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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-550/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm

42

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-5304

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF Advanced: до 5.0.0.21

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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-549/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm

43

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-5303

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF Advanced: до версии 5.0.0.21

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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-548/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm

44

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-5302

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF Advanced: до версии 5.0.0.21

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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-547/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm

45

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-5301

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

Уязвимый продукт: Power PDF Advanced: до версии 5.0.0.21

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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-546/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm

46

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-30373

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF Advanced: до версии 5.0.0.21

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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-557/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm

47

Краткое описание: Выполнение произвольного кода в Composer

Идентификатор уязвимости: CVE-2024-35241

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

Уязвимый продукт: composer: с версии 2.0.0 по 2.7.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-11 / 2024-06-11

Ссылки на источник:

- http://github.com/composer/composer/security/advisories/GHSA-47f6-5gq3-vx9c
- http://github.com/composer/composer/commit/b93fc6ca437da35ae73d667d0618749c763b67d4
- http://github.com/composer/composer/commit/ee28354ca8d33c15949ad7de2ce6656ba3f68704

Краткое описание: Выполнение произвольного кода в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-28038

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: e-STUDIO 908: все версии
e-STUDIO 1058: все версии
e-STUDIO 1208: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Переполнение буфера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93051062/index.html
- http://www.toshibatec.com/information/20240531_02.html

Краткое описание: Чтение локальных файлов в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-33605

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

Уязвимый продукт: e-STUDIO 908: все версии
e-STUDIO 1058: все версии
e-STUDIO 1208: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

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: 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: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93051062/index.html
- http://www.toshibatec.com/information/20240531_02.html

Краткое описание: Потеря целостности в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-33610

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: e-STUDIO 908: все версии
e-STUDIO 1058: все версии
e-STUDIO 1208: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Потеря целостности

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: 9.1 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: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93051062/index.html
- http://www.toshibatec.com/information/20240531_02.html

Краткое описание: Получение конфиденциальной информации в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-35244

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

Уязвимый продукт: e-STUDIO 908: все версии
e-STUDIO 1058: все версии
e-STUDIO 1208: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Использование жестко закодированных учетных данных

Последствия эксплуатации: Получение конфиденциальной информации

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: 9.1 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: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93051062/index.html
- http://www.toshibatec.com/information/20240531_02.html

Краткое описание: Получение конфиденциальной информации в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-36248

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

Уязвимый продукт: e-STUDIO 908: все версии
e-STUDIO 1058: все версии
e-STUDIO 1208: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Использование жестко закодированных учетных данных

Последствия эксплуатации: Получение конфиденциальной информации

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: 9.1 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: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93051062/index.html
- http://www.toshibatec.com/information/20240531_02.html

53

Краткое описание: Межсайтовый скриптинг в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-36249

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

Уязвимый продукт: e-STUDIO 908: все версии
e-STUDIO 1058: все версии
e-STUDIO 1208: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93051062/index.html
- http://www.toshibatec.com/information/20240531_02.html

Краткое описание: Отказ в обслуживании в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-36251

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: e-STUDIO 908: все версии
e-STUDIO 1058: все версии
e-STUDIO 1208: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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: 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: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93051062/index.html
- http://www.toshibatec.com/information/20240531_02.html

55

Краткое описание: Выполнение произвольного кода в Emerson Ovation

Идентификатор уязвимости: CVE-2022-30267

Идентификатор программной ошибки: CWE-345 Некорректная проверка достоверности данных

Уязвимый продукт: Ovation: 3.8.0 Feature Pack 1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-158-02
- https://bdu.fstec.ru/vul/2022-03852

56

Краткое описание: Выполнение произвольного кода в Fuji Electric Monitouch V-SFT

Идентификатор уязвимости: CVE-2024-5597

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

Уязвимый продукт: Monitouch V-SFT: до 6.2.3.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-151-02
- http://www.zerodayinitiative.com/advisories/ZDI-24-564/
- https://bdu.fstec.ru/vul/2024-04473

57

Краткое описание: Чтение локальных файлов в Apache OFBiz

Идентификатор уязвимости: CVE-2024-36104

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

Уязвимый продукт: OFBiz: с версии 18.12.01 по 18.12.13

Категория уязвимого продукта: Прикладное программное обеспечение

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: 9.1 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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://issues.apache.org/jira/browse/OFBIZ-13092
- http://lists.apache.org/thread/sv0xr8b1j7mmh5p37yldy9vmnzbodz2o

58

Краткое описание: Получение конфиденциальной информации в Westermo EDW-100

Идентификатор уязвимости: CVE-2024-36081

Идентификатор программной ошибки: CWE-522 Недостаточно надежная защита учетных данных

Уязвимый продукт: EDW-100: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Ссылки на источник:

- http://www.westermo.com/-/media/Files/Cyber-security/westermo_sa_EDW-100_24-05.pdf
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-151-04

Краткое описание: Отказ в обслуживании в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-36254

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: e-STUDIO 908: все версии
e-STUDIO 1058: все версии
e-STUDIO 1208: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

59

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: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93051062/index.html
- http://www.toshibatec.com/information/20240531_02.html

Краткое описание: Обход безопасности в Johnson Controls Software House iStar Pro Door Controller and ICU

Идентификатор уязвимости: CVE-2024-32752

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

Уязвимый продукт: Software House iStar Pro Door Controller: все версии
ICU: 6.9.2.25888

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

60

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

Оценка CVSSv3: 9.1 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: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2024/jci-psa-2024-06.pdf
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-158-04

61

Краткое описание: Выполнение произвольного кода в Git for Windows

Идентификатор уязвимости: CVE-2024-32004

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

Уязвимый продукт: Git for Windows: 2.0.0 - 2.45.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://github.com/git-for-windows/git/releases/tag/v2.43.4.windows.1
- http://github.com/git-for-windows/git/releases/tag/v2.44.1.windows.1
- https://bdu.fstec.ru/vul/2024-04093

Краткое описание: Выполнение произвольного кода в Fuji Electric Monitouch V-SFT

Идентификатор уязвимости: CVE-2024-34171

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Monitouch V-SFT: до 6.2.3.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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.

62

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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-151-02
- http://www.zerodayinitiative.com/advisories/ZDI-24-535/
- http://www.zerodayinitiative.com/advisories/ZDI-24-534/
- http://www.zerodayinitiative.com/advisories/ZDI-24-533/
- http://www.zerodayinitiative.com/advisories/ZDI-24-532/
- http://www.zerodayinitiative.com/advisories/ZDI-24-530/
- https://bdu.fstec.ru/vul/2024-04285

63

Краткое описание: Получение конфиденциальной информации в Westermo EDW-100

Идентификатор уязвимости: CVE-2024-36080

Идентификатор программной ошибки: CWE-259 Использование жестко закодированного пароля

Уязвимый продукт: EDW-100: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Получение конфиденциальной информации

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

Ссылки на источник:

- http://www.westermo.com/-/media/Files/Cyber-security/westermo_sa_EDW-100_24-05.pdf
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-151-04

64

Краткое описание: Обход безопасности в Emerson Ovation

Идентификатор уязвимости: CVE-2022-29966

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

Уязвимый продукт: Ovation: 3.8.0 Feature Pack 1

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: 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: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-158-02
- https://bdu.fstec.ru/vul/2022-03839

65

Краткое описание: Выполнение произвольного кода в Apache Wicket

Идентификатор уязвимости: CVE-2024-36522

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

Уязвимый продукт: Apache Wicket: 9.0.0 - 10.0.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Некорректная проверка входных 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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://lists.apache.org/thread/lm84pzcbh34rsv9spz9cm24g4jspzbqg
- http://lists.apache.org/thread/k0ppy7vjc9h0ohl7j43wqyt9c6ywjytw
- https://bdu.fstec.ru/vul/2024-04429

66

Краткое описание: Запись локальных файлов в Git

Идентификатор уязвимости: CVE-2024-32002

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

Уязвимый продукт: Git: с версии 2.0.0 по 2.45.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

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

Оценка CVSSv3: 9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://github.com/git/git/security/advisories/GHSA-8h77-4q3w-gfgv
- https://bdu.fstec.ru/vul/2024-03872

67

Краткое описание: Запись локальных файлов в Git for Windows

Идентификатор уязвимости: CVE-2024-32002

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

Уязвимый продукт: Git for Windows: с версии 2.0.0 по 2.45.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

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

Оценка CVSSv3: 9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://github.com/git-for-windows/git/releases/tag/v2.43.4.windows.1
- http://github.com/git-for-windows/git/releases/tag/v2.44.1.windows.1
- https://bdu.fstec.ru/vul/2024-03872

68

Краткое описание: Выполнение произвольного кода в libarchive

Идентификатор уязвимости: CVE-2024-26256

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

Уязвимый продукт: libarchive: с версии 3.0 по 3.7.3

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.zerodayinitiative.com/blog/2024/4/17/cve-2024-20697-windows-libarchive-remote-code-execution-vulnerability
- http://github.com/libarchive/libarchive/releases/tag/v3.7.4
- https://bdu.fstec.ru/vul/2024-02924

Краткое описание: Чтение локальных файлов в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2024-28995

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

Уязвимый продукт: Serv-U FTP Server: с версии 15.1 по 15.4.2 Hotfix 1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Чтение локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-07 / 2024-06-07

Ссылки на источник:

- http://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28995

70

Краткое описание: Выполнение произвольного кода в Fuji Electric Monitouch V-SFT

Идентификатор уязвимости: CVE-2024-5271

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Monitouch V-SFT: до версии 6.2.3.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-151-02
- http://www.zerodayinitiative.com/advisories/ZDI-24-531/
- https://bdu.fstec.ru/vul/2024-04344

Краткое описание: Выполнение произвольного кода в Cisco Firepower Management Center

Идентификатор уязвимости: CVE-2024-20360

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

Уязвимый продукт: Cisco Firepower Management Center (FMC): до версии 7.0.2.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

71

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: 2024-05-22 / 2024-05-22

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-04131

72

Краткое описание: Выполнение произвольного кода в Cisco Crosswork Network Services Orchestrator

Идентификатор уязвимости: CVE-2024-20366

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

Уязвимый продукт: Crosswork Network Services Orchestrator: 5.0 - 6.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-hcc-priv-esc-OWBWCs5D
- https://bdu.fstec.ru/vul/2024-03965

73

Краткое описание: Перезапись произвольных файлов в FortiSandbox

Идентификатор уязвимости: CVE-2024-31491

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

Уязвимый продукт: FortiSandbox: 4.2.0 - 4.4.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Перезапись произвольных файлов

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

Оценка CVSSv3: 8.8 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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-24-054
- https://bdu.fstec.ru/vul/2024-03866