НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-05-26.1 | 26 мая 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-33236	MXsecurity	Сетевой	SB	2023-05-26	✓
2	Критическая	CVE-2023-33010	Zyxel firewalls	Сетевой	ACE	2023-05-25	✓
3	Критическая	CVE-2023-33009	Zyxel firewalls	Сетевой	ACE	2023-05-25	✓
4	Критическая	CVE-2023-2868	Barracuda Email Security Gateway (ESG)	Сетевой	ACE	2023-05-25	✓
5	Критическая	CVE-2023-1424	Mitsubishi Electric MELSEC iQ-F Series	Сетевой	ACE	2023-05-24	✓
6	Критическая	CVE-2023-0856	Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers	Сетевой	ACE	2023-05-24	✓
7	Критическая	CVE-2023-0855	Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers	Сетевой	ACE	2023-05-24	✓
8	Критическая	CVE-2023-0853	Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers	Сетевой	ACE	2023-05-24	✓
9	Критическая	CVE-2023-0852	Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers	Сетевой	ACE	2023-05-24	✓
10	Критическая	CVE-2023-0854	Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers	Сетевой	ACE	2023-05-24	✓

11	Критическая	CVE-2023-0851	Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers	Сетевой	ACE	2023-05-24	✓
12	Критическая	CVE-2023-31047	Ubuntu	Сетевой	WLF	2023-05-25	✓
13	Высокая	CVE-2023-27530	Public Cloud Module	Сетевой	DoS	2023-05-25	✓
14	Высокая	CVE-2023-24038	Ubuntu	Сетевой	DoS	2023-05-25	✓
15	Критическая	CVE-2023-22741	Debian Linux	Сетевой	ACE	2023-05-24	✓
16	Высокая	CVE-2022-47516	Debian Linux	Сетевой	DoS	2023-05-24	✓
17	Критическая	CVE-2022-31003	Debian Linux	Сетевой	ACE	2023-05-24	✓
18	Высокая	CVE-2022-31002	Debian Linux	Сетевой	DoS	2023-05-24	✓
19	Высокая	CVE-2022-31001	Debian Linux	Сетевой	DoS	2023-05-24	✓
20	Критическая	CVE-2023-2868	Email Security Gateway (ESG)	Сетевой	ACE	2023-05-25	✓
21	Критическая	CVE-2021-3918	Ubuntu	Сетевой	ACE	2023-05-24	✓
22	Высокая	CVE-2023-32159	PDF-XChange Editor	Локальный	ACE	2023-05-22	✓
23	Высокая	CVE-2023-32160	PDF-XChange Editor	Локальный	ACE	2023-05-22	✓
24	Высокая	CVE-2023-32161	PDF-XChange Editor	Локальный	ACE	2023-05-22	✓
25	Высокая	CVE-2023-32158	PDF-XChange Editor	Локальный	ACE	2023-05-22	✓

26	Высокая	CVE-2023-28756	cflinuxfs3	Сетевой	RLF	2023-05-22	✓
27	Высокая	CVE-2023-28755	cflinuxfs3	Сетевой	OAF	2023-05-22	✓
28	Критическая	CVE-2023-1133	Delta Electronics InfraSuite Device Master	Сетевой	ACE	2023-05-23	✓
29	Высокая	CVE-2023-1142	Delta Electronics InfraSuite Device Master	Сетевой	RLF	2023-05-23	✓
30	Высокая	CVE-2023-1145	InfraSuite Device Master	Локальный	RLF	2023-05-23	✓
31	Высокая	CVE-2023-1139	Delta Electronics InfraSuite Device Master	Сетевой	ACE	2023-05-23	✓
32	Критическая	CVE-2023-1136	Delta Electronics InfraSuite Device Master	Сетевой	Не определено	2023-05-23	✓
33	Высокая	CVE-2023-1143	Delta Electronics InfraSuite Device Master	Сетевой	ACE	2023-05-23	✓
34	Высокая	CVE-2023-1144	Delta Electronics InfraSuite Device Master	Сетевой	PE	2023-05-23	✓
35	Критическая	CVE-2023-1140	Delta Electronics InfraSuite Device Master	Сетевой	ACE	2023-05-23	✓
36	Высокая	CVE-2023-1138	Delta Electronics InfraSuite Device Master	Сетевой	SB	2023-05-23	✓
37	Высокая	CVE-2023-1135	Delta Electronics InfraSuite Device Master	Локальный	ACE	2023-05-23	✓
38	Высокая	CVE-2023-32336	IBM InfoSphere Information Server	Смежная сеть	ACE	2023-05-23	✗

39	Высокая	CVE-2023-33005	Jenkins WSO2 Oauth plugin	Сетевой	OSI	2023-05-22	✗

1

Краткое описание: Обход безопасности в MXsecurity

Идентификатор уязвимости: CVE-2023-33236

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

Уязвимый продукт: MXsecurity: 1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-26 / 2023-05-26

Ссылки на источник:

- http://www.moxa.com/en/support/product-support/security-advisory/mxsecurity-command-injection-and-hardcoded-credential-vulnerabilities
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-145-01
- http://www.zerodayinitiative.com/advisories/ZDI-23-720/
- https://bdu.fstec.ru/vul/2023-01149

Краткое описание: Выполнение произвольного кода в Zyxel firewalls

Идентификатор уязвимости: CVE-2023-33010

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

Уязвимый продукт: Zyxel firewalls:
ATP series: 4.32 - 5.36 Patch 1
USG FLEX series: 4.50 - 5.36 Patch 1
USG FLEX 50W: 4.25 - 5.36 Patch 1
USG20W-VPN: 4.25 - 5.36 Patch 1
VPN series: 4.30 - 5.36 Patch 1
ZyWALL: 4.25 - 4.73 Patch 1
USG series: 4.25 - 4.73 Patch 1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

2

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-25 / 2023-05-25

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls
- https://bdu.fstec.ru/vul/2023-02796

Краткое описание: Выполнение произвольного кода в Zyxel firewalls

Идентификатор уязвимости: CVE-2023-33009

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

Уязвимый продукт: Zyxel firewalls:
ATP series: 4.32 - 5.36 Patch 1
USG FLEX series: 4.50 - 5.36 Patch 1
USG FLEX 50W: 4.25 - 5.36 Patch 1
USG20W-VPN: 4.25 - 5.36 Patch 1
VPN series: 4.30 - 5.36 Patch 1
ZyWALL: 4.25 - 4.73 Patch 1
USG series: 4.25 - 4.73 Patch 1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

3

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-25 / 2023-05-25

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls
- https://bdu.fstec.ru/vul/2023-02797

4

Краткое описание: Выполнение произвольного кода в Barracuda Email Security Gateway (ESG)

Идентификатор уязвимости: CVE-2023-2868

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

Уязвимый продукт: Barracuda Email Security Gateway (ESG): 5.1.3 - 9.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-25 / 2023-05-25

Ссылки на источник:

- http://status.barracuda.com/incidents/34kx82j5n4q9
- http://www.barracuda.com/company/legal/esg-vulnerability

5

Краткое описание: Выполнение произвольного кода в Mitsubishi Electric MELSEC iQ-F Series

Идентификатор уязвимости: CVE-2023-1424

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

Уязвимый продукт: Mitsubishi Electric MELSEC iQ-F Series:
MELSEC iQ-F FX5U: 1.220
MELSEC iQ-F FX5UC: 1.220
MELSEC iQ-F FX5UC-32MT/DS-TS: 1.220
MELSEC iQ-F FX5UC-32MT/DSS-TS: 1.220
MELSEC iQ-F FX5UC-32MR/DS-TS: 1.220

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-143-03
- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-003_en.pdf
- http://jvn.jp/vu/JVNVU94650413
- https://bdu.fstec.ru/vul/2023-02792

6

Краткое описание: Выполнение произвольного кода в Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers

Идентификатор уязвимости: CVE-2023-0856

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers:
i-SENSYS X C1127P: все версии
i-SENSYS C1127iF: все версии
i-SENSYS X C1127i: все версии
i-SENSYS MF746Cx: все версии
i-SENSYS MF744CDW: все версии
i-SENSYS MF742CDW: все версии
i-SENSYS MF645Cx: все версии
i-SENSYS MF643CDW: все версии
i-SENSYS MF641Cw: все версии
i-SENSYS LBP664Cx: все версии
i-SENSYS LBP633Cdw: все версии
i-SENSYS LBP623Cdw: все версии
i-SENSYS LBP621Cw: все версии

Категория уязвимого продукта: Периферийное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://psirt.canon/advisory-information/cp2023-001/
- http://www.canon-europe.com/support/product-security-latest-news/

7

Краткое описание: Выполнение произвольного кода в Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers

Идентификатор уязвимости: CVE-2023-0855

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers:
i-SENSYS X C1127P: все версии
i-SENSYS C1127iF: все версии
i-SENSYS X C1127i: все версии
i-SENSYS MF746Cx: все версии
i-SENSYS MF744CDW: все версии
i-SENSYS MF742CDW: все версии
i-SENSYS MF645Cx: все версии
i-SENSYS MF643CDW: все версии
i-SENSYS MF641Cw: все версии
i-SENSYS LBP664Cx: все версии
i-SENSYS LBP633Cdw: все версии
i-SENSYS LBP623Cdw: все версии
i-SENSYS LBP621Cw: все версии

Категория уязвимого продукта: Периферийное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://psirt.canon/advisory-information/cp2023-001/
- http://www.canon-europe.com/support/product-security-latest-news/

8

Краткое описание: Выполнение произвольного кода в Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers

Идентификатор уязвимости: CVE-2023-0853

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers:
i-SENSYS X C1127P: все версии
i-SENSYS C1127iF: все версии
i-SENSYS X C1127i: все версии
i-SENSYS MF746Cx: все версии
i-SENSYS MF744CDW: все версии
i-SENSYS MF742CDW: все версии
i-SENSYS MF645Cx: все версии
i-SENSYS MF643CDW: все версии
i-SENSYS MF641Cw: все версии
i-SENSYS LBP664Cx: все версии
i-SENSYS LBP633Cdw: все версии
i-SENSYS LBP623Cdw: все версии
i-SENSYS LBP621Cw: все версии

Категория уязвимого продукта: Периферийное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://psirt.canon/advisory-information/cp2023-001/
- http://www.canon-europe.com/support/product-security-latest-news/

9

Краткое описание: Выполнение произвольного кода в Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers

Идентификатор уязвимости: CVE-2023-0852

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers:
i-SENSYS X C1127P: все версии
i-SENSYS C1127iF: все версии
i-SENSYS X C1127i: все версии
i-SENSYS MF746Cx: все версии
i-SENSYS MF744CDW: все версии
i-SENSYS MF742CDW: все версии
i-SENSYS MF645Cx: все версии
i-SENSYS MF643CDW: все версии
i-SENSYS MF641Cw: все версии
i-SENSYS LBP664Cx: все версии
i-SENSYS LBP633Cdw: все версии
i-SENSYS LBP623Cdw: все версии
i-SENSYS LBP621Cw: все версии

Категория уязвимого продукта: Периферийное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://psirt.canon/advisory-information/cp2023-001/
- http://www.canon-europe.com/support/product-security-latest-news/

10

Краткое описание: Выполнение произвольного кода в Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers

Идентификатор уязвимости: CVE-2023-0854

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

Уязвимый продукт: Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers:
i-SENSYS X C1127P: все версии
i-SENSYS C1127iF: все версии
i-SENSYS X C1127i: все версии
i-SENSYS MF746Cx: все версии
i-SENSYS MF744CDW: все версии
i-SENSYS MF742CDW: все версии
i-SENSYS MF645Cx: все версии
i-SENSYS MF643CDW: все версии
i-SENSYS MF641Cw: все версии
i-SENSYS LBP664Cx: все версии
i-SENSYS LBP633Cdw: все версии
i-SENSYS LBP623Cdw: все версии
i-SENSYS LBP621Cw: все версии

Категория уязвимого продукта: Периферийное 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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://psirt.canon/advisory-information/cp2023-001/
- http://www.canon-europe.com/support/product-security-latest-news/

11

Краткое описание: Выполнение произвольного кода в Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers

Идентификатор уязвимости: CVE-2023-0851

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

Уязвимый продукт: Canon Office/Small Office Multifunction Printers, Laser Printers and Inkjet Printers:
i-SENSYS X C1127P: все версии
i-SENSYS C1127iF: все версии
i-SENSYS X C1127i: все версии
i-SENSYS MF746Cx: все версии
i-SENSYS MF744CDW: все версии
i-SENSYS MF742CDW: все версии
i-SENSYS MF645Cx: все версии
i-SENSYS MF643CDW: все версии
i-SENSYS MF641Cw: все версии
i-SENSYS LBP664Cx: все версии
i-SENSYS LBP633Cdw: все версии
i-SENSYS LBP623Cdw: все версии
i-SENSYS LBP621Cw: все версии

Категория уязвимого продукта: Периферийное 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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://psirt.canon/advisory-information/cp2023-001/
- http://www.canon-europe.com/support/product-security-latest-news/

12

Краткое описание: Запись локальных файлов в Ubuntu

Идентификатор уязвимости: CVE-2023-31047

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

Уязвимый продукт: Ubuntu: 16.04, 14.04
python-django-doc (Ubuntu package): до Ubuntu Pro
python-django (Ubuntu package): до Ubuntu Pro
python3-django (Ubuntu package): до Ubuntu Pro

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

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-25 / 2023-05-25

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6054-2

13

Краткое описание: Отказ в обслуживании в Public Cloud Module

Идентификатор уязвимости: CVE-2023-27530

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Public Cloud Module: 15-SP4
Server Applications Module: 15-SP4
SUSE Linux Enterprise Server for SAP Applications 15: SP4
SUSE Linux Enterprise Server 15: SP4
SUSE Linux Enterprise Real Time 15: SP4
SUSE Linux Enterprise High Performance Computing 15: SP4
SUSE Manager Retail Branch Server: 4.3
SUSE Manager Server: 4.3
SUSE Manager Proxy: 4.3
openSUSE Leap: 15.4
rmt-server-config: до 2.13-150400.3.12.1
rmt-server: до 2.13-150400.3.12.1
rmt-server-pubcloud: до 2.13-150400.3.12.1
rmt-server-debugsource: до 2.13-150400.3.12.1
rmt-server-debuginfo: до 2.13-150400.3.12.1

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-25 / 2023-05-25

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20232295-1/
- https://bdu.fstec.ru/vul/2023-01752

Краткое описание: Отказ в обслуживании в Ubuntu

Идентификатор уязвимости: CVE-2023-24038

Идентификатор программной ошибки: CWE-185 Некорректные регулярные выражения

Уязвимый продукт: Ubuntu: 22.10, 22.04, 20.04, 18.04, 16.04, 14.04
libhtml-stripscripts-perl (Ubuntu package): до Ubuntu Pro

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-25 / 2023-05-25

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6100-1
- https://bdu.fstec.ru/vul/2023-01007

15

Краткое описание: Выполнение произвольного кода в Debian Linux

Идентификатор уязвимости: CVE-2023-22741

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Debian Linux: все версии
sofia-sip (Debian package): до 1.12.11+20110422.1-2.1+deb11u1

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

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://www.debian.org/security/2023/dsa-5410

16

Краткое описание: Отказ в обслуживании в Debian Linux

Идентификатор уязвимости: CVE-2022-47516

Идентификатор программной ошибки: CWE-617 Несанкционированный вызов утверждения

Уязвимый продукт: Debian Linux: все версии
sofia-sip (Debian package): до 1.12.11+20110422.1-2.1+deb11u1

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

Способ эксплуатации: Отправка специально сформированного запроса.

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://www.debian.org/security/2023/dsa-5410

17

Краткое описание: Выполнение произвольного кода в Debian Linux

Идентификатор уязвимости: CVE-2022-31003

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

Уязвимый продукт: Debian Linux: все версии
sofia-sip (Debian package): до 1.12.11+20110422.1-2.1+deb11u1

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://www.debian.org/security/2023/dsa-5410

18

Краткое описание: Отказ в обслуживании в Debian Linux

Идентификатор уязвимости: CVE-2022-31002

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Debian Linux: все версии
sofia-sip (Debian package): до 1.12.11+20110422.1-2.1+deb11u1

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://www.debian.org/security/2023/dsa-5410

19

Краткое описание: Отказ в обслуживании в Debian Linux

Идентификатор уязвимости: CVE-2022-31001

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Debian Linux: все версии
sofia-sip (Debian package): до 1.12.11+20110422.1-2.1+deb11u1

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://www.debian.org/security/2023/dsa-5410

Краткое описание: Выполнение произвольного кода в Email Security Gateway (ESG)

Идентификатор уязвимости: CVE-2023-2868

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

Уязвимый продукт: Email Security Gateway (ESG): 5.1.3 - 9.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка 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.

20

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-25 / 2023-05-25

Ссылки на источник:

- http://status.barracuda.com/incidents/34kx82j5n4q9
- http://www.barracuda.com/company/legal/esg-vulnerability

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2021-3918

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

Уязвимый продукт: Ubuntu: 20.04, 18.04
node-json-schema (Ubuntu package): до 0.2.3-1+deb10u1build0.18.04.1

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

Способ эксплуатации: Отправка 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.

21

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-24 / 2023-05-24

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6103-1
- https://bdu.fstec.ru/vul/2022-04683

22

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor

Идентификатор уязвимости: CVE-2023-32159

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 9.5.368.0

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-641/
- http://www.tracker-software.com/product/pdf-xchange-editor/history

23

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor

Идентификатор уязвимости: CVE-2023-32160

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 9.5.368.0

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-642/
- http://www.tracker-software.com/product/pdf-xchange-editor/history

24

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor

Идентификатор уязвимости: CVE-2023-32161

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 9.5.368.0

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-643/
- http://www.tracker-software.com/product/pdf-xchange-editor/history

25

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor

Идентификатор уязвимости: CVE-2023-32158

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 9.5.368.0

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-640/
- http://www.tracker-software.com/product/pdf-xchange-editor/history

26

Краткое описание: Чтение локальных файлов в cflinuxfs3

Идентификатор уязвимости: CVE-2023-28756

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

Уязвимый продукт: cflinuxfs3: 0.0.0 - 0.365.0

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://github.com/cloudfoundry/cflinuxfs3/releases/tag/0.366.0
- https://bdu.fstec.ru/vul/2023-02020

27

Краткое описание: Перезапись произвольных файлов в cflinuxfs3

Идентификатор уязвимости: CVE-2023-28755

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

Уязвимый продукт: cflinuxfs3: 0.0.0 - 0.365.0

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://github.com/cloudfoundry/cflinuxfs3/releases/tag/0.366.0

28

Краткое описание: Выполнение произвольного кода в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-1133

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.5

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02
- http://www.zerodayinitiative.com/advisories/ZDI-23-683/
- https://bdu.fstec.ru/vul/2023-01818

Краткое описание: Чтение локальных файлов в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-1142

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

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.5

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.

29

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02
- http://www.zerodayinitiative.com/advisories/ZDI-23-682/
- https://bdu.fstec.ru/vul/2023-02143

Краткое описание: Чтение локальных файлов в InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-1145

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: InfraSuite Device Master: до 1.0.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

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.

30

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02
- http://www.zerodayinitiative.com/advisories/ZDI-23-681/
- https://bdu.fstec.ru/vul/2023-01933

Краткое описание: Выполнение произвольного кода в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-1139

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.5

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.

31

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02
- http://www.zerodayinitiative.com/advisories/ZDI-23-680/
- https://bdu.fstec.ru/vul/2023-01941

Краткое описание: Уязвимость в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-1136

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Не определено

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.

32

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02
- http://www.zerodayinitiative.com/advisories/ZDI-23-679/
- https://bdu.fstec.ru/vul/2023-02111

Краткое описание: Выполнение произвольного кода в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-1143

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

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

33

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02
- http://www.zerodayinitiative.com/advisories/ZDI-23-676/
- https://bdu.fstec.ru/vul/2023-02085

Краткое описание: Повышение привилегий в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-1144

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

34

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02
- http://www.zerodayinitiative.com/advisories/ZDI-23-675/
- https://bdu.fstec.ru/vul/2023-02110

Краткое описание: Выполнение произвольного кода в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-1140

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.5

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.

35

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02
- http://www.zerodayinitiative.com/advisories/ZDI-23-674/
- https://bdu.fstec.ru/vul/2023-01564

Краткое описание: Обход безопасности в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-1138

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

36

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02
- http://www.zerodayinitiative.com/advisories/ZDI-23-673/
- https://bdu.fstec.ru/vul/2023-02087

Краткое описание: Выполнение произвольного кода в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-1135

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.5

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.

37

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-080-02
- http://www.zerodayinitiative.com/advisories/ZDI-23-686/
- https://bdu.fstec.ru/vul/2023-02089

38

Краткое описание: Выполнение произвольного кода в IBM InfoSphere Information Server

Идентификатор уязвимости: CVE-2023-32336

Идентификатор программной ошибки: CWE-16 Уязвимости, связанные с конфигурацией

Уязвимый продукт: IBM InfoSphere Information Server: 11.7 - 11.7.1.4 Service pack 1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-23 / 2023-05-23

Ссылки на источник:

- http://www.ibm.com/support/pages/node/6995879
- http://exchange.xforce.ibmcloud.com/vulnerabilities/255285
- http://www.ibm.com/support/pages/node/6454607

39

Краткое описание: Получение конфиденциальной информации в Jenkins WSO2 Oauth plugin

Идентификатор уязвимости: CVE-2023-33005

Идентификатор программной ошибки: CWE-384 Фиксация сессии

Уязвимый продукт: Jenkins WSO2 Oauth plugin: 1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://jenkins.io/security/advisory/2023-05-16/