НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-01-31.1 | 31 января 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-0402	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	OAF	2024-01-26	✓
2	Высокая	CVE-2023-43609	Emerson Rosemount GC370XA, GC700XA, GC1500XA	Смежная сеть	DoS	2024-01-31	✓
3	Высокая	CVE-2023-51761	Emerson Rosemount GC370XA, GC700XA, GC1500XA	Смежная сеть	SB	2024-01-31	✓
4	Высокая	CVE-2023-49716	Emerson Rosemount GC370XA, GC700XA, GC1500XA	Смежная сеть	ACE	2024-01-31	✓
5	Критическая	CVE-2023-46687	Emerson Rosemount GC370XA, GC700XA, GC1500XA	Сетевой	ACE	2024-01-31	✓
6	Критическая	CVE-2023-6943	Mitsubishi Electric FA Engineering Software Products	Сетевой	ACE	2024-01-31	✗
7	Высокая	CVE-2023-6942	Mitsubishi Electric FA Engineering Software Products	Сетевой	SB	2024-01-31	✗
8	Высокая	CVE-2024-21916	Rockwell Automation ControlLogix and GuardLogix	Сетевой	DoS	2024-01-31	✓
9	Критическая	CVE-2024-23625	D-Link DAP-1650	Смежная сеть	ACE	2024-01-30	✗
10	Критическая	CVE-2024-23624	D-Link DAP-1650	Смежная сеть	ACE	2024-01-30	✗
11	Высокая	CVE-2024-0911	GNU indent	Сетевой	ACE	2024-01-26	✗

1

Краткое описание: Перезапись произвольных файлов в GitLab Community Edition (CE) and Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2024-0402

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

Уязвимый продукт: Gitlab Community Edition: 16.0.0 - 16.8.0
GitLab Enterprise Edition: 16.0.0 - 16.8.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/
- https://bdu.fstec.ru/vul/2024-00724

2

Краткое описание: Отказ в обслуживании в Emerson Rosemount GC370XA, GC700XA, GC1500XA

Идентификатор уязвимости: CVE-2023-43609

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: GC370XA: 4.1.5
GC700XA: 4.1.5
GC1500XA: 4.1.5

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-31 / 2024-01-31

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-030-01
- http://www.emerson.com/documents/automation/security-notification-emerson-gas-chromatographs-cyber-security-notification-icsa-24-030-01-en-10103910.pdf

Краткое описание: Обход безопасности в Emerson Rosemount GC370XA, GC700XA, GC1500XA

Идентификатор уязвимости: CVE-2023-51761

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: GC370XA: 4.1.5
GC700XA: 4.1.5
GC1500XA: 4.1.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: обход безопасности

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

Оценка CVSSv3: 8.3 AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-31 / 2024-01-31

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-030-01
- http://www.emerson.com/documents/automation/security-notification-emerson-gas-chromatographs-cyber-security-notification-icsa-24-030-01-en-10103910.pdf

Краткое описание: Выполнение произвольного кода в Emerson Rosemount GC370XA, GC700XA, GC1500XA

Идентификатор уязвимости: CVE-2023-49716

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

Уязвимый продукт: GC370XA: 4.1.5
GC700XA: 4.1.5
GC1500XA: 4.1.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

4

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

Оценка CVSSv3: 8.0 AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-31 / 2024-01-31

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-030-01
- http://www.emerson.com/documents/automation/security-notification-emerson-gas-chromatographs-cyber-security-notification-icsa-24-030-01-en-10103910.pdf

Краткое описание: Выполнение произвольного кода в Emerson Rosemount GC370XA, GC700XA, GC1500XA

Идентификатор уязвимости: CVE-2023-46687

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

Уязвимый продукт: GC370XA: 4.1.5
GC700XA: 4.1.5
GC1500XA: 4.1.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

5

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-31 / 2024-01-31

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-030-01
- http://www.emerson.com/documents/automation/security-notification-emerson-gas-chromatographs-cyber-security-notification-icsa-24-030-01-en-10103910.pdf

6

Краткое описание: Выполнение произвольного кода в Mitsubishi Electric FA Engineering Software Products

Идентификатор уязвимости: CVE-2023-6943

Идентификатор программной ошибки: CWE-470 Использование внешних входных данных для выбора класса или кода ("небезопасное отражение")

Уязвимый продукт: EZSocket: 3.0
FR Configurator2: все версии
GT Designer3 Version1(GOT1000): все версии
GT Designer3 Version1(GOT2000): все версии
GX Works2: 1.11M
GX Works3: все версии
MELSOFT Navigator: 1.04E
MT Works2: все версии
MX Component: 4.00A
MX OPC Server DA: все версии
MX OPC Server UA: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Вызов функции с путем к вредоносной библиотеке

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-31 / 2024-01-31

Ссылки на источник:

- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-020_en.pdf
- http://jvn.jp/vu/JVNVU95103362
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-030-02

Краткое описание: Обход безопасности в Mitsubishi Electric FA Engineering Software Products

Идентификатор уязвимости: CVE-2023-6942

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

Уязвимый продукт: EZSocket: 3.0
FR Configurator2: все версии
GT Designer3 Version1(GOT1000): все версии
GT Designer3 Version1(GOT2000): все версии
GX Works2: 1.11M
GX Works3: все версии
MELSOFT Navigator: 1.04E
MT Works2: все версии
MX Component: 4.00A
MX OPC Server DA: все версии
MX OPC Server UA: все версии

7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: обход безопасности

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

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: 2024-01-31 / 2024-01-31

Ссылки на источник:

- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-020_en.pdf
- http://jvn.jp/vu/JVNVU95103362
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-030-02

8

Краткое описание: Отказ в обслуживании в Rockwell Automation ControlLogix and GuardLogix

Идентификатор уязвимости: CVE-2024-21916

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

Уязвимый продукт: ControlLogix 5570: 20.011
ControlLogix 5570 redundant: 20.054_kit1
GuardLogix 5570: 20.011

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-31 / 2024-01-31

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-030-05

9

Краткое описание: Выполнение произвольного кода в D-Link DAP-1650

Идентификатор уязвимости: CVE-2024-23625

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

Уязвимый продукт: DAP-1650: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 9.6 AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-30 / 2024-01-30

Ссылки на источник:

- http://blog.exodusintel.com/2024/01/25/d-link-dap-1650-subscribe-callback-command-injection-vulnerability/

10

Краткое описание: Выполнение произвольного кода в D-Link DAP-1650

Идентификатор уязвимости: CVE-2024-23624

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

Уязвимый продукт: DAP-1650: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 9.6 AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-30 / 2024-01-30

Ссылки на источник:

- http://blog.exodusintel.com/2024/01/25/d-link-dap-1650-gena-cgi-subscribe-command-injection-vulnerability/

11

Краткое описание: Выполнение произвольного кода в GNU indent

Идентификатор уязвимости: CVE-2024-0911

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

Уязвимый продукт: Indent: 2.1.0 - 2.2.13

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://bugzilla.redhat.com/show_bug.cgi?id=2260399
- http://bugzilla.redhat.com/show_bug.cgi?id=2259883