НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-11-07.1 | 7 ноября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-1720	Bitrix24	Сетевой	XSS\CSS	2023-11-01	✓
2	Высокая	CVE-2023-1719	Bitrix24	Сетевой	ACE	2023-11-01	✓
3	Высокая	CVE-2023-1718	Bitrix24	Сетевой	DoS	2023-11-01	✓
4	Критическая	CVE-2023-1717	Bitrix24	Сетевой	XSS\CSS	2023-11-01	✓
5	Критическая	CVE-2023-1716	Bitrix24	Сетевой	XSS\CSS	2023-11-01	✓
6	Критическая	CVE-2023-1715	Bitrix24	Сетевой	XSS\CSS	2023-11-01	✓
7	Высокая	CVE-2023-1714	Bitrix24	Сетевой	ACE	2023-11-01	✓
8	Высокая	CVE-2023-1713	Bitrix24	Сетевой	ACE	2023-11-01	✓
9	Критическая	CVE-2023-4699	Mitsubishi Electric MELSEC Series	Сетевой	DoS	2023-11-03	✗
10	Высокая	CVE-2023-4967	Citrix NetScaler ADC and NetScaler Gateway	Сетевой	DoS	2023-10-11	✓

1

Краткое описание: Межсайтовый скриптинг в Bitrix24

Идентификатор уязвимости: CVE-2023-1720

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

Уязвимый продукт: Bitrix24: 22.0.300

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-01 / 2023-11-01

Ссылки на источник:

- https://starlabs.sg/advisories/23/23-1720/
- https://bdu.fstec.ru/vul/2023-07458

2

Краткое описание: Выполнение произвольного кода в Bitrix24

Идентификатор уязвимости: CVE-2023-1719

Идентификатор программной ошибки: CWE-454 Инициализация доверенных переменных или хранилищ данных извне

Уязвимый продукт: Bitrix24: 22.0.300

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: 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: 2023-11-01 / 2023-11-01

Ссылки на источник:

- https://starlabs.sg/advisories/23/23-1719/
- https://bdu.fstec.ru/vul/2023-07459

3

Краткое описание: Отказ в обслуживании в Bitrix24

Идентификатор уязвимости: CVE-2023-1718

Идентификатор программной ошибки: CWE-835 Бесконечный цикл (зацикливание)

Уязвимый продукт: Bitrix24: 22.0.300

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

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: 2023-11-01 / 2023-11-01

Ссылки на источник:

- https://starlabs.sg/advisories/23/23-1718/
- https://bdu.fstec.ru/vul/2023-07460

4

Краткое описание: Межсайтовый скриптинг в Bitrix24

Идентификатор уязвимости: CVE-2023-1717

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

Уязвимый продукт: Bitrix24: 22.0.300

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-01 / 2023-11-01

Ссылки на источник:

- https://starlabs.sg/advisories/23/23-1717/
- https://bdu.fstec.ru/vul/2023-07461

5

Краткое описание: Межсайтовый скриптинг в Bitrix24

Идентификатор уязвимости: CVE-2023-1716

Идентификатор программной ошибки: CWE-83 Некорректная нейтрализация сценариев в атрибутах на веб-страницах

Уязвимый продукт: Bitrix24: 22.0.300

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-01 / 2023-11-01

Ссылки на источник:

- https://starlabs.sg/advisories/23/23-1715/
- https://bdu.fstec.ru/vul/2023-07462

6

Краткое описание: Межсайтовый скриптинг в Bitrix24

Идентификатор уязвимости: CVE-2023-1715

Идентификатор программной ошибки: CWE-83 Некорректная нейтрализация сценариев в атрибутах на веб-страницах

Уязвимый продукт: Bitrix24: 22.0.300

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-01 / 2023-11-01

Ссылки на источник:

- https://starlabs.sg/advisories/23/23-1715/
- https://bdu.fstec.ru/vul/2023-07463

7

Краткое описание: Выполнение произвольного кода в Bitrix24

Идентификатор уязвимости: CVE-2023-1714

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

Уязвимый продукт: Bitrix24: 22.0.300

Категория уязвимого продукта: Прикладное программное обеспечение

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.

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: 2023-11-01 / 2023-11-01

Ссылки на источник:

- https://starlabs.sg/advisories/23/23-1714/
- https://bdu.fstec.ru/vul/2023-07457

8

Краткое описание: Выполнение произвольного кода в Bitrix24

Идентификатор уязвимости: CVE-2023-1713

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

Уязвимый продукт: Bitrix24: 22.0.300

Категория уязвимого продукта: Прикладное программное обеспечение

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.

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: 2023-11-01 / 2023-11-01

Ссылки на источник:

- https://starlabs.sg/advisories/23/23-1713/
- https://bdu.fstec.ru/vul/2023-07464

9

Краткое описание: Отказ в обслуживании в Mitsubishi Electric MELSEC Series

Идентификатор уязвимости: CVE-2023-4699

Идентификатор программной ошибки: CWE-345 Некорректная проверка достоверности данных

Уязвимый продукт: Mitsubishi Electric MELSEC Series:
MELSEC-F FX3U: все версии
MELSEC-F FX3U-32MR/UA1: все версии
MELSEC-F FX3U-64MS/ES: все версии
MELSEC-F FX3UC: все версии
MELSEC-F FX3UC-16MR/D-T: все версии
MELSEC-F FX3UC-16MR/DS-T: все версии
MELSEC-F FX3UC-32MT-LT: все версии
MELSEC-F FX3UC-32MT-LT-2: все версии
MELSEC-F FX3UC-16MT/D-P4: все версии
MELSEC-F FX3UC-16MT/DSS-P4: все версии
MELSEC-F FX3G: все версии
MELSEC-F FX3GC-32MT/D: все версии
MELSEC-F FX3GC-32MT/DSS: все версии
MELSEC-F FX3GE: все версии
MELSEC-F FX3GA: все версии
MELSEC-F FX3S: все версии
MELSEC-F FX3S-30My/z-2AD: все версии
MELSEC-F FX3SA-xMy-CM: все версии
MELSEC iQ-F FX5U: все версии
MELSEC iQ-F FX5UC: все версии
MELSEC iQ-F FX5UC-32MT/DS-TS: все версии
MELSEC iQ-F FX5UC-32MT/DSS-TS: все версии
MELSEC iQ-F FX5UC-32MR/DS-TS: все версии
MELSEC iQ-F FX5UJ: все версии
MELSEC iQ-F FX5S: все версии
MELSEC-F FX3U-64MR/UA1: все версии
MELSEC-F FX3U-32MS/ES: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: отказ в обслуживании

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:N/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-03 / 2023-11-03

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-306-03
- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-013_en.pdf

10

Краткое описание: Отказ в обслуживании в Citrix NetScaler ADC and NetScaler Gateway

Идентификатор уязвимости: CVE-2023-4967

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

Уязвимый продукт: Citrix NetScaler ADC and NetScaler Gateway:
Citrix Netscaler ADC: 12.1-55.289 - 14.1-4.42
Citrix NetScaler Gateway: 12.1-55.289 - 14.1-4.42

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-11 / 2023-10-11

Ссылки на источник:

- http://support.citrix.com/article/CTX579459