НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-06-21.1 | 21 июня 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-26801	LB-LINK Wireless Routers	Сетевой	ACE	2023-06-21	✗
2	Высокая	CVE-2023-28703	ASUS Routers	Сетевой	ACE	2023-06-20	✓
3	Высокая	CVE-2022-46871	ASUS Routers	Сетевой	ACE	2023-06-20	✓
4	Высокая	CVE-2023-28702	ASUS Routers	Сетевой	ACE	2023-06-20	✓
5	Критическая	CVE-2023-27992	Zyxel NAS products	Сетевой	ACE	2023-06-20	✓
6	Высокая	CVE-2023-29349	Microsoft ODBC Driver for SQL Server on Windows	Локальный	ACE	2023-06-15	✓
7	Высокая	CVE-2023-32028	Microsoft OLE DB Driver	Локальный	ACE	2023-06-15	✓
8	Высокая	CVE-2023-32025	Microsoft ODBC Driver for SQL Server on Windows	Локальный	ACE	2023-06-15	✓
9	Высокая	CVE-2023-32026	Microsoft ODBC Driver for SQL Server on Windows	Локальный	ACE	2023-06-15	✓
10	Высокая	CVE-2023-32027	Microsoft ODBC Driver for SQL Server on Windows	Локальный	ACE	2023-06-15	✓
11	Высокая	CVE-2023-29356	Microsoft ODBC Driver for SQL Server on Windows	Локальный	ACE	2023-06-15	✓
12	Критическая	CVE-2023-29297	Adobe Commerce (formerly Magento Commerce)	Сетевой	XSS\CSS	2023-06-16	✓

13	Высокая	CVE-2023-22248	Adobe Commerce (formerly Magento Commerce)	Сетевой	SB	2023-06-16	✓
14	Критическая	CVE-2022-43546	SIEMENS POWER METER SICAM Q200	Сетевой	ACE	2023-06-16	✓
15	Критическая	CVE-2022-43545	SIEMENS POWER METER SICAM Q200	Сетевой	ACE	2023-06-16	✓
16	Критическая	CVE-2022-23219	Siemens SIMATIC S7-1500 TM MFP - BIOS	Сетевой	ACE	2023-06-16	✗
17	Критическая	CVE-2022-43439	SIEMENS POWER METER SICAM Q200	Сетевой	ACE	2023-06-16	✓
18	Критическая	CVE-2022-23218	Siemens SIMATIC S7-1500 TM MFP - BIOS	Сетевой	ACE	2023-06-16	✗
19	Высокая	CVE-2022-4378	Siemens SIMATIC S7-1500 TM MFP - BIOS	Локальный	PE	2023-06-16	✗
20	Критическая	CVE-2022-1292	Siemens SINAMICS PERFECT HARMONY GH180 6SR5	Сетевой	ACE	2023-06-16	✓
21	Высокая	CVE-2022-23308	Siemens SINAMICS PERFECT HARMONY GH180 6SR5	Сетевой	OSI	2023-06-16	✓
22	Высокая	CVE-2022-36946	Siemens SINAMICS PERFECT HARMONY GH180 6SR5	Сетевой	DoS	2023-06-16	✓
23	Высокая	CVE-2023-29321	Adobe Animate	Локальный	ACE	2023-06-15	✓

1

Краткое описание: Выполнение произвольного кода в LB-LINK Wireless Routers

Идентификатор уязвимости: CVE-2023-26801

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

Уязвимый продукт: LB-LINK Wireless Routers:
BL-AC1900: 1.0.1 - 1.0.1
BL-WR9000: 2.4.9 - 2.4.9
BL-X26: 1.2.5 - 1.2.5
BL-LTE300: 1.0.8 - 1.0.8

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-21 / 2023-06-21

Ссылки на источник:

- http://github.com/winmt/my-vuls/tree/main/LB-LINK%20BL-AC1900%2C%20BL-WR9000%2C%20BL-X26%20and%20BL-LTE300%20Wireless%20Routers
- http://www.broadcom.com/support/security-center/attacksignatures/detail?asid=34211
- https://bdu.fstec.ru/vul/2023-02970

2

Краткое описание: Выполнение произвольного кода в ASUS Routers

Идентификатор уязвимости: CVE-2023-28703

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: ASUS Routers:
TUF-AX5400: до 3.0.0.4.388.23285
TUF-AX6000: до 3.0.0.4.388.31927
RT-AX58U: до 3.0.0.4.388.23403
RT-AX82U: до 3.0.0.4.388.23285
RT-AX86S: до 3.0.0.4.388.23285
RT-AX86U: до 3.0.0.4.388.23285
RT-AX86U PRO: до 3.0.0.4.388.23285
ZenWiFi XT8_V2: до 3.0.0.4.388.23285
ZenWiFi XT8: до 3.0.0.4.388.23285
ZenWiFi XT9: до 3.0.0.4.388.23285
GS-AX3000: до 1.4.8.3
GS-AX5400: до 3.0.0.4.388.23012
GT-AX11000: до 3.0.0.4.388.23285
GT-AX6000: до 3.0.0.4.388.23285
GT-AXE11000: до 3.0.0.4.388.23482
GT-AXE11000 PRO: до 3.0.0.4.388.23285
GT-AXE16000: до 3.0.0.4.388.23012
GT6: до 3.0.0.4.388.23145
RT-AX3000: до 3.0.0.4.388.23403

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: 7.2 AV:N/AC:L/PR:H/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: 2023-06-20 / 2023-06-20

Ссылки на источник:

- http://www.asus.com/content/asus-product-security-advisory/#06/19/2023
- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230620

3

Краткое описание: Выполнение произвольного кода в ASUS Routers

Идентификатор уязвимости: CVE-2022-46871

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

Уязвимый продукт: ASUS Routers:
TUF-AX5400: до 3.0.0.4.388.23285
TUF-AX6000: до 3.0.0.4.388.31927
RT-AX58U: до 3.0.0.4.388.23403
RT-AX82U: до 3.0.0.4.388.23285
RT-AX86S: до 3.0.0.4.388.23285
RT-AX86U: до 3.0.0.4.388.23285
RT-AX86U PRO: до 3.0.0.4.388.23285
ZenWiFi XT8_V2: до 3.0.0.4.388.23285
ZenWiFi XT8: до 3.0.0.4.388.23285
ZenWiFi XT9: до 3.0.0.4.388.23285
GS-AX3000: до 1.4.8.3
GS-AX5400: до 3.0.0.4.388.23012
GT-AX11000: до 3.0.0.4.388.23285
GT-AX6000: до 3.0.0.4.388.23285
GT-AXE11000: до 3.0.0.4.388.23482
GT-AXE11000 PRO: до 3.0.0.4.388.23285
GT-AXE16000: до 3.0.0.4.388.23012
GT6: до 3.0.0.4.388.23145
RT-AX3000: до 3.0.0.4.388.23403

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-20 / 2023-06-20

Ссылки на источник:

- http://www.asus.com/content/asus-product-security-advisory/#06/19/2023
- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230620
- https://bdu.fstec.ru/vul/2023-00385

4

Краткое описание: Выполнение произвольного кода в ASUS Routers

Идентификатор уязвимости: CVE-2023-28702

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

Уязвимый продукт: ASUS Routers:
TUF-AX5400: до 3.0.0.4.388.23285
TUF-AX6000: до 3.0.0.4.388.31927
RT-AX58U: до 3.0.0.4.388.23403
RT-AX82U: до 3.0.0.4.388.23285
RT-AX86S: до 3.0.0.4.388.23285
RT-AX86U: до 3.0.0.4.388.23285
RT-AX86U PRO: до 3.0.0.4.388.23285
ZenWiFi XT8_V2: до 3.0.0.4.388.23285
ZenWiFi XT8: до 3.0.0.4.388.23285
ZenWiFi XT9: до 3.0.0.4.388.23285
GS-AX3000: до 1.4.8.3
GS-AX5400: до 3.0.0.4.388.23012
GT-AX11000: до 3.0.0.4.388.23285
GT-AX6000: до 3.0.0.4.388.23285
GT-AXE11000: до 3.0.0.4.388.23482
GT-AXE11000 PRO: до 3.0.0.4.388.23285
GT-AXE16000: до 3.0.0.4.388.23012
GT6: до 3.0.0.4.388.23145
RT-AX3000: до 3.0.0.4.388.23403

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-20 / 2023-06-20

Ссылки на источник:

- http://www.asus.com/content/asus-product-security-advisory/#06/19/2023
- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230620

5

Краткое описание: Выполнение произвольного кода в Zyxel NAS products

Идентификатор уязвимости: CVE-2023-27992

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

Уязвимый продукт: Zyxel NAS products:
NAS326: 5.21(AAZF.13)C0 - 5.21(AAZF.13)C0
NAS540: 5.21(AATB.10)C0 - 5.21(AATB.10)C0
NAS542: 5.21(ABAG.10)C0 - 5.21(ABAG.10)C0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-06-20 / 2023-06-20

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-pre-authentication-command-injection-vulnerability-in-nas-products

6

Краткое описание: Выполнение произвольного кода в Microsoft ODBC Driver for SQL Server on Windows

Идентификатор уязвимости: CVE-2023-29349

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft ODBC Driver for SQL Server on Windows: 17 for SQL Server - 18.2.2
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.2.2
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.2.2
OLE DB Driver: 18.0.2 - 19.3.0
Microsoft SQL Server: 2019 15.0.2000.5 - 2022 RC1 16.0.950.9

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-06-15 / 2023-06-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29349

7

Краткое описание: Выполнение произвольного кода в Microsoft OLE DB Driver

Идентификатор уязвимости: CVE-2023-32028

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft OLE DB Driver: 18.0.2 - 19.3.0
Microsoft SQL Server: 2019 15.0.2000.5 - 2022 RC1 16.0.950.9

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-06-15 / 2023-06-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-32028

8

Краткое описание: Выполнение произвольного кода в Microsoft ODBC Driver for SQL Server on Windows

Идентификатор уязвимости: CVE-2023-32025

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.2.2
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.2.2
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.2.2
Microsoft SQL Server: 2019 15.0.2000.5 - 2022 RC1 16.0.950.9

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-06-15 / 2023-06-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-32025

9

Краткое описание: Выполнение произвольного кода в Microsoft ODBC Driver for SQL Server on Windows

Идентификатор уязвимости: CVE-2023-32026

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.2.2
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.2.2
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.2.2
Microsoft SQL Server: 2019 15.0.2000.5 - 2022 RC1 16.0.950.9

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-06-15 / 2023-06-15

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-32026

10

Краткое описание: Выполнение произвольного кода в Microsoft ODBC Driver for SQL Server on Windows

Идентификатор уязвимости: CVE-2023-32027

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.2.2
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.2.2
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.2.2
Microsoft SQL Server: 2019 15.0.2000.5 - 2022 RC1 16.0.950.9

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-06-15 / 2023-06-15

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-32027

11

Краткое описание: Выполнение произвольного кода в Microsoft ODBC Driver for SQL Server on Windows

Идентификатор уязвимости: CVE-2023-29356

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.2.2
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.2.2
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.2.2
Microsoft SQL Server: 2019 15.0.2000.5 - 2022 RC1 16.0.950.9

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-06-15 / 2023-06-15

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29356

Краткое описание: Межсайтовый скриптинг в Adobe Commerce (formerly Magento Commerce)

Идентификатор уязвимости: CVE-2023-29297

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

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.3.7 - 2.4.6
Magento Open Source: 2.3.7 - 2.4.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Межсайтовый скриптинг

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/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: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb23-35.html

13

Краткое описание: Обход безопасности в Adobe Commerce (formerly Magento Commerce)

Идентификатор уязвимости: CVE-2023-22248

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.3.7 - 2.4.6
Magento Open Source: 2.3.7 - 2.4.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса авторизации

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: 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: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb23-35.html

14

Краткое описание: Выполнение произвольного кода в SIEMENS POWER METER SICAM Q200

Идентификатор уязвимости: CVE-2022-43546

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SIEMENS POWER METER SICAM Q200: до 2.70

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-887249.txt
- https://bdu.fstec.ru/vul/2022-07320

15

Краткое описание: Выполнение произвольного кода в SIEMENS POWER METER SICAM Q200

Идентификатор уязвимости: CVE-2022-43545

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SIEMENS POWER METER SICAM Q200: до 2.70

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-887249.txt
- https://bdu.fstec.ru/vul/2022-07317

16

Краткое описание: Выполнение произвольного кода в Siemens SIMATIC S7-1500 TM MFP - BIOS

Идентификатор уязвимости: CVE-2022-23219

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

Уязвимый продукт: Siemens SIMATIC S7-1500 TM MFP - BIOS: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-831302.txt
- https://bdu.fstec.ru/vul/2022-01633

17

Краткое описание: Выполнение произвольного кода в SIEMENS POWER METER SICAM Q200

Идентификатор уязвимости: CVE-2022-43439

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SIEMENS POWER METER SICAM Q200: до 2.70

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-887249.txt
- https://bdu.fstec.ru/vul/2022-07322

18

Краткое описание: Выполнение произвольного кода в Siemens SIMATIC S7-1500 TM MFP - BIOS

Идентификатор уязвимости: CVE-2022-23218

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

Уязвимый продукт: Siemens SIMATIC S7-1500 TM MFP - BIOS: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-831302.txt
- https://bdu.fstec.ru/vul/2022-01632

19

Краткое описание: Повышение привилегий в Siemens SIMATIC S7-1500 TM MFP - BIOS

Идентификатор уязвимости: CVE-2022-4378

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Siemens SIMATIC S7-1500 TM MFP - BIOS: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Повышение привилегий

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

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: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-831302.txt
- https://bdu.fstec.ru/vul/2022-07336

20

Краткое описание: Выполнение произвольного кода в Siemens SINAMICS PERFECT HARMONY GH180 6SR5

Идентификатор уязвимости: CVE-2022-1292

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

Уязвимый продукт: Siemens SINAMICS PERFECT HARMONY GH180 6SR5: все версии
Siemens SINAMICS SL150: все версии
Siemens SINAMICS GL150: все версии
Siemens SCALANCE S615: до 7.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-942865.txt
- https://bdu.fstec.ru/vul/2022-03181

Краткое описание: Получение конфиденциальной информации в Siemens SINAMICS PERFECT HARMONY GH180 6SR5

Идентификатор уязвимости: CVE-2022-23308

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Siemens SINAMICS PERFECT HARMONY GH180 6SR5: все версии
Siemens SINAMICS SL150: все версии
Siemens SINAMICS GL150: все версии
Siemens SCALANCE S615: до 7.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-942865.txt
- https://bdu.fstec.ru/vul/2022-01453

Краткое описание: Отказ в обслуживании в Siemens SINAMICS PERFECT HARMONY GH180 6SR5

Идентификатор уязвимости: CVE-2022-36946

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Siemens SINAMICS PERFECT HARMONY GH180 6SR5: все версии
Siemens SINAMICS SL150: все версии
Siemens SINAMICS GL150: все версии
Siemens SCALANCE S615: до 7.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2023-06-16 / 2023-06-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-942865.txt
- https://bdu.fstec.ru/vul/2022-04686

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2023-29321

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Animate: 15.2.1.95 - 23.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-06-15 / 2023-06-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/animate/apsb23-36.html