НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-07-24.1 | 24 июля 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-33876	Foxit PDF	Сетевой	ACE	2023-07-20	✓
2	Высокая	CVE-2023-32664	Foxit PDF	Сетевой	ACE	2023-07-20	✓
3	Высокая	CVE-2023-33866	Foxit PDF	Сетевой	ACE	2023-07-20	✓
4	Высокая	CVE-2023-27379	Foxit PDF Reader for Windows	Сетевой	ACE	2023-07-20	✓
5	Высокая	CVE-2023-28744	Foxit PDF	Сетевой	ACE	2023-07-20	✓
6	Критическая	CVE-2023-38204	Adobe ColdFusion	Сетевой	ACE	2023-07-20	✓
7	Высокая	CVE-2023-38205	Adobe ColdFusion	Сетевой	ACE	2023-07-20	✓
8	Высокая	CVE-2023-38098	NETGEAR NMS300	Сетевой	WLF	2023-07-19	✓
9	Высокая	CVE-2023-38099	NETGEAR NMS300	Сетевой	ACE	2023-07-19	✓
10	Высокая	CVE-2023-38100	NETGEAR NMS300	Сетевой	ACE	2023-07-19	✓
11	Высокая	CVE-2023-38102	NETGEAR NMS300	Сетевой	SB	2023-07-19	✓
12	Высокая	CVE-2023-38095	NETGEAR NMS300	Сетевой	RLF	2023-07-19	✓
13	Высокая	CVE-2023-34123	SonicWall GMS и SonicWall Analytics	Сетевой	SB	2023-07-13	✓

14	Критическая	CVE-2023-33308	FortiOS и FortiProxy	Сетевой	ACE	2023-07-11	✓
15	Критическая	CVE-2023-37706	Tenda FH1203	Сетевой	DoS	2023-07-10	✓
16	Критическая	CVE-2023-37712	Tenda AC1206 Tenda F1202 Tenda FH1202	Сетевой	ACE	2023-07-10	✓
17	Критическая	CVE-2023-37703	Tenda FH1203	Сетевой	DoS	2023-07-10	✓
18	Критическая	CVE-2023-37145	TOTOLINK LR350	Сетевой	ACE	2023-07-07	✓
19	Критическая	CVE-2023-37710	Tenda AC1206	Сетевой	ACE	2023-07-10	✓
20	Критическая	CVE-2023-37170	TOTOLINK A3300R	Сетевой	ACE	2023-07-07	✓
21	Критическая	CVE-2023-37702	Tenda FH1203	Сетевой	DoS	2023-07-10	✓
22	Критическая	CVE-2023-37711	Tenda AC1206	Сетевой	ACE	2023-07-10	✓
23	Критическая	CVE-2023-37704	Tenda FH1203	Сетевой	DoS	2023-07-10	✓
24	Критическая	CVE-2023-37700	Tenda FH1203	Сетевой	DoS	2023-07-10	✓
25	Критическая	CVE-2023-37704	Tenda FH1203	Сетевой	DoS	2023-07-10	✓
26	Критическая	CVE-2023-37701	Tenda FH1203	Сетевой	DoS	2023-07-10	✓
27	Критическая	CVE-2023-37707	Tenda FH1203	Сетевой	DoS	2023-07-10	✓
28	Критическая	CVE-2023-37144	Tenda AC10	Сетевой	PE	2023-07-07	✓

29	Высокая	CVE-2023-28985	Juniper MX и SRX	Сетевой	DoS	2023-07-14	✓
30	Высокая	CVE-2023-36831	Juniper Junos OS	Сетевой	DoS	2023-07-16	✓
31	Высокая	CVE-2023-36832	Juniper Junos OS	Сетевой	DoS	2023-07-16	✓
32	Высокая	CVE-2023-36835	Juniper Junos OS	Сетевой	DoS	2023-07-16	✓
33	Высокая	CVE-2023-34137	SonicWall GMS и Analytics	Сетевой	ACE	2023-07-18	✓
34	Высокая	CVE-2023-34134	SonicWall GMS и Analytics	Сетевой	OSI	2023-07-18	✓
35	Высокая	CVE-2023-34133	SonicWall GMS и Analytics	Сетевой	ACE	2023-07-18	✓
36	Высокая	CVE-2023-34127	SonicWall GMS и Analytics	Сетевой	ACE	2023-07-18	✓
37	Высокая	CVE-2023-34124	SonicWall GMS и Analytics	Сетевой	ACE	2023-07-18	✓
38	Критическая	CVE-2023-3638	GeoVision GV-ADR2701	Сетевой	SB	2023-07-19	✗
39	Критическая	CVE-2023-28121	WordPress-плагин WooCommerce Payments	Сетевой	PE	2023-07-03	✓
40	Критическая	CVE-2023-3519	Citrix ADC и Citrix Gateway	Сетевой	ACE	2023-07-18	✓
41	Высокая	CVE-2023-3467	Citrix ADC и Citrix Gateway	Смежная сеть	PE	2023-07-18	✓
42	Высокая	CVE-2023-3466	Citrix ADC и Citrix Gateway	Сетевой	XSS\CSS	2023-07-18	✓

43	Высокая	CVE-2023-34141	Zyxel firewalls and WLAN controllers	Смежная сеть	ACE	2023-07-18	✓
44	Высокая	CVE-2023-34139	Zyxel firewalls and WLAN controllers	Смежная сеть	ACE	2023-07-18	✓
45	Высокая	CVE-2023-34138	Zyxel firewalls and WLAN controllers	Смежная сеть	ACE	2023-07-18	✓
46	Высокая	CVE-2023-33012	Zyxel firewalls and WLAN controllers	Смежная сеть	ACE	2023-07-18	✓
47	Высокая	CVE-2023-33011	Zyxel firewalls and WLAN controllers	Смежная сеть	ACE	2023-07-18	✓
48	Высокая	CVE-2023-28767	Zyxel firewalls and WLAN controllers	Смежная сеть	ACE	2023-07-18	✓

1

Краткое описание: Выполнение произвольного кода в Foxit PDF

Идентификатор уязвимости: CVE-2023-33876

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

Уязвимый продукт: Foxit PDF:
Foxit PDF Reader for Windows 10.0.0.35798 - 12.1.2.15332
Foxit PDF Editor (formerly Foxit PhantomPDF) 10.0.0.35798 - 12.1.2.15332

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-20 / 2023-07-20

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+12.1.3+and+Foxit+PDF+Editor+12.1.32023-07-19+00%3A00%3A00

2

Краткое описание: Выполнение произвольного кода в Foxit PDF

Идентификатор уязвимости: CVE-2023-32664

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

Уязвимый продукт: Foxit PDF:
Foxit PDF Reader for Windows 10.0.0.35798 - 12.1.2.15332
Foxit PDF Editor (formerly Foxit PhantomPDF) 10.0.0.35798 - 12.1.2.15332

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-20 / 2023-07-20

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+12.1.3+and+Foxit+PDF+Editor+12.1.32023-07-19+00%3A00%3A00

3

Краткое описание: Выполнение произвольного кода в Foxit PDF

Идентификатор уязвимости: CVE-2023-33866

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

Уязвимый продукт: Foxit PDF:
Foxit PDF Reader for Windows 10.0.0.35798 - 12.1.2.15332
Foxit PDF Editor (formerly Foxit PhantomPDF) 10.0.0.35798 - 12.1.2.15332

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-20 / 2023-07-20

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+12.1.3+and+Foxit+PDF+Editor+12.1.32023-07-19+00%3A00%3A00

4

Краткое описание: Выполнение произвольного кода в Foxit PDF Reader for Windows

Идентификатор уязвимости: CVE-2023-27379

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

Уязвимый продукт: Foxit PDF Reader for Windows: 10.0.0.35798 - 12.1.2.15332
Foxit PDF Editor (formerly Foxit PhantomPDF): 10.0.0.35798 - 12.1.2.15332

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-20 / 2023-07-20

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+12.1.3+and+Foxit+PDF+Editor+12.1.32023-07-19+00%3A00%3A00

5

Краткое описание: Выполнение произвольного кода в Foxit PDF

Идентификатор уязвимости: CVE-2023-28744

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

Уязвимый продукт: Foxit PDF:
Foxit PDF Reader for Windows 10.0.0.35798 - 12.1.2.15332
Foxit PDF Editor (formerly Foxit PhantomPDF) 10.0.0.35798 - 12.1.2.15332

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-20 / 2023-07-20

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+12.1.3+and+Foxit+PDF+Editor+12.1.32023-07-19+00%3A00%3A00

6

Краткое описание: Выполнение произвольного кода в Adobe ColdFusion

Идентификатор уязвимости: CVE-2023-38204

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Adobe ColdFusion: 2018 - 2023 Update 2

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: 2023-07-20 / 2023-07-20

Ссылки на источник:

- http://helpx.adobe.com/security/products/coldfusion/apsb23-47.html

7

Краткое описание: Выполнение произвольного кода в Adobe ColdFusion

Идентификатор уязвимости: CVE-2023-38205

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Adobe ColdFusion: 2018 - 2023 Update 2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-07-20 / 2023-07-20

Ссылки на источник:

- http://helpx.adobe.com/security/products/coldfusion/apsb23-47.html

8

Краткое описание: Запись локальных файлов в NETGEAR NMS300

Идентификатор уязвимости: CVE-2023-38098

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

Уязвимый продукт: NETGEAR NMS300: до 1.7.0.20

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2023-07-19 / 2023-07-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-918/
- http://kb.netgear.com/000065707/Security-Advisory-for-Multiple-Vulnerabilities-on-the-ProSAFE-Network-Management-System-PSV-2023-0024-PSV-2023-0025

9

Краткое описание: Выполнение произвольного кода в NETGEAR NMS300

Идентификатор уязвимости: CVE-2023-38099

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

Уязвимый продукт: NETGEAR NMS300: до 1.7.0.20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-07-19 / 2023-07-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-917/
- http://kb.netgear.com/000065707/Security-Advisory-for-Multiple-Vulnerabilities-on-the-ProSAFE-Network-Management-System-PSV-2023-0024-PSV-2023-0025

10

Краткое описание: Выполнение произвольного кода в NETGEAR NMS300

Идентификатор уязвимости: CVE-2023-38100

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

Уязвимый продукт: NETGEAR NMS300: до 1.7.0.20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-07-19 / 2023-07-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-916/
- http://kb.netgear.com/000065707/Security-Advisory-for-Multiple-Vulnerabilities-on-the-ProSAFE-Network-Management-System-PSV-2023-0024-PSV-2023-0025

11

Краткое описание: Обход безопасности в NETGEAR NMS300

Идентификатор уязвимости: CVE-2023-38102

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: NETGEAR NMS300: до 1.7.0.20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

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: 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: 2023-07-19 / 2023-07-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-914/
- http://kb.netgear.com/000065707/Security-Advisory-for-Multiple-Vulnerabilities-on-the-ProSAFE-Network-Management-System-PSV-2023-0024-PSV-2023-0025

Краткое описание: Чтение локальных файлов в NETGEAR NMS300

Идентификатор уязвимости: CVE-2023-38095

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

Уязвимый продукт: NETGEAR NMS300: до 1.7.0.20

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных 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.

12

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: 2023-07-19 / 2023-07-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-921/
- http://kb.netgear.com/000065707/Security-Advisory-for-Multiple-Vulnerabilities-on-the-ProSAFE-Network-Management-System-PSV-2023-0024-PSV-2023-0025

13

Краткое описание: Обход безопасности в SonicWall GMS и SonicWall Analytics

Идентификатор уязвимости: CVE-2023-34123

Идентификатор программной ошибки: CWE-321 Использование жестко закодированного ключа шифрования

Уязвимый продукт: SonicWall GMS и SonicWall Analytics:
GMS: 9.3.2-SP1
Analytics: 2.5.0.4-R7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование жестко закодированного пароля

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:N/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0010
- https://www.sonicwall.com/support/notices/230710150218060

14

Краткое описание: Выполнение произвольного кода в FortiOS и FortiProxy

Идентификатор уязвимости: CVE-2023-33308

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: FortiOS и FortiProxy:
OS: 7.0.0 - 7.2.3
Proxy: 7.0.0 - 7.2.2

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: 2023-07-11 / 2023-07-11

Ссылки на источник:

- http://fortiguard.fortinet.com/psirt/FG-IR-23-183
- https://bdu.fstec.ru/vul/2023-03690

Краткое описание: Отказ в обслуживании в Tenda FH1203

Идентификатор уязвимости: CVE-2023-37706

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda FH1203: V2.0.1.6

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: 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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/6903

Краткое описание: Выполнение произвольного кода в Tenda AC1206 Tenda F1202 Tenda FH1202

Идентификатор уязвимости: CVE-2023-37712

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC1206
Tenda F1202
Tenda FH1202:
AC1206 V15.03.06.23, F1202 V1.2.0.20(408), FH1202: V1.2.0.20(408)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

16

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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/fromSetIpBind

Краткое описание: Отказ в обслуживании в Tenda FH1203

Идентификатор уязвимости: CVE-2023-37703

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda FH1203: V2.0.1.6

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

17 **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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/6907

18

Краткое описание: Выполнение произвольного кода в TOTOLINK LR350

Идентификатор уязвимости: CVE-2023-37145

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

Уязвимый продукт: TOTOLINK LR350: V9.3.5u.6369_B20220309

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: 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: 2023-07-07 / 2023-07-12

Ссылки на источник:

- https://github.com/DaDong-G/Vulnerability_info/blob/main/TOTOLINK/lr350/1/Readme.md

19

Краткое описание: Выполнение произвольного кода в Tenda AC1206

Идентификатор уязвимости: CVE-2023-37710

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC1206: V15.03.06.23

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: 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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/fromSetWirelessRepeat

Краткое описание: Выполнение произвольного кода в TOTOLINK A3300R

Идентификатор уязвимости: CVE-2023-37170

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

Уязвимый продукт: TOTOLINK A3300R: V17.0.0cu.557_B20221024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

20

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: 2023-07-07 / 2023-07-13

Ссылки на источник:

- https://github.com/kafroc/Vuls/tree/main/TOTOLINK/A3300R/cmdi_1

Краткое описание: Отказ в обслуживании в Tenda FH1203

Идентификатор уязвимости: CVE-2023-37702

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda FH1203: V2.0.1.6

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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: 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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/6801

Краткое описание: Выполнение произвольного кода в Tenda AC1206

Идентификатор уязвимости: CVE-2023-37711

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC1206: V15.03.06.23

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.

22

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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/saveParentControlInfo

Краткое описание: Отказ в обслуживании в Tenda FH1203

Идентификатор уязвимости: CVE-2023-37704

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda FH1203: V2.0.1.6

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.

23

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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/6901

Краткое описание: Отказ в обслуживании в Tenda FH1203

Идентификатор уязвимости: CVE-2023-37700

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda FH1203: V2.0.1.6

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.

24

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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/6905

Краткое описание: Отказ в обслуживании в Tenda FH1203

Идентификатор уязвимости: CVE-2023-37704

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda FH1203: V2.0.1.6

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: 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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/6901

Краткое описание: Отказ в обслуживании в Tenda FH1203

Идентификатор уязвимости: CVE-2023-37701

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda FH1203: V2.0.1.6

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/6908

Краткое описание: Отказ в обслуживании в Tenda FH1203

Идентификатор уязвимости: CVE-2023-37707

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda FH1203: V2.0.1.6

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

27 **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: 2023-07-10 / 2023-07-13

Ссылки на источник:

- https://github.com/FirmRec/IoT-Vulns/tree/main/tenda/6904

28

Краткое описание: Повышение привилегий в Tenda AC10

Идентификатор уязвимости: CVE-2023-37144

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

Уязвимый продукт: Tenda AC10: v15.03.06.26

Категория уязвимого продукта: Телекоммуникационное оборудование

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.

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: 2023-07-07 / 2023-07-12

Ссылки на источник:

- https://github.com/DaDong-G/Vulnerability_info/blob/main/ac10_command_injection/Readme.md

Краткое описание: Отказ в обслуживании в Juniper MX и SRX

Идентификатор уязвимости: CVE-2023-28985

Идентификатор программной ошибки: CWE-1286 Некорректная проверка правильности синтаксиса входных данных

Уязвимый продукт: Juniper MX и SRX: до версии 22.4R2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 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: 2023-07-14 / 2023-07-14

Ссылки на источник:

- https://supportportal.juniper.net/JSA71662

30

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-36831

Идентификатор программной ошибки: CWE-755 Некорректная обработка исключений

Уязвимый продукт: Juniper Junos OS: до 23.1R1

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-16 / 2023-07-16

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-SRX-Series-jbuf-memory-leak-when-SSL-Proxy-and-UTM-Web-Filtering-is-applied-CVE-2023-36831

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-36832

Идентификатор программной ошибки: CWE-754 Некорректная проверка наличия нестандартных условий или исключений

Уязвимый продукт: Juniper Junos OS: до 23.1R1

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

31 **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: 2023-07-16 / 2023-07-16

Ссылки на источник:

- http://supportportal.juniper.net/JSA71639

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-36835

Идентификатор программной ошибки: CWE-754 Некорректная проверка наличия нестандартных условий или исключений

Уязвимый продукт: Juniper Junos OS: до 22.4R1

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

32 **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: 2023-07-16 / 2023-07-16

Ссылки на источник:

- http://supportportal.juniper.net/JSA71642

Краткое описание: Выполнение произвольного кода в SonicWall GMS и Analytics

Идентификатор уязвимости: CVE-2023-34137

Идентификатор программной ошибки: CWE-305 Обход аутентификации с помощью стороннего недостатка

Уязвимый продукт: SonicWall GMS и Analytics:
SonicWall GMS: 9.3.2-SP1 - 9.3.2-SP1
SonicWall Analytics: 2.5.0.4-R7 - 2.5.0.4-R7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0010
- http://www.sonicwall.com/support/knowledge-base/urgent-security-notice-sonicwall-gms-analytics-impacted-by-suite-of-vulnerabilities/230710150218060/

Краткое описание: Получение конфиденциальной информации в SonicWall GMS и Analytics

Идентификатор уязвимости: CVE-2023-34134

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

Уязвимый продукт: SonicWall GMS и Analytics:
SonicWall GMS: 9.3.2-SP1 - 9.3.2-SP1
SonicWall Analytics: 2.5.0.4-R7 - 2.5.0.4-R7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0010
- http://www.sonicwall.com/support/knowledge-base/urgent-security-notice-sonicwall-gms-analytics-impacted-by-suite-of-vulnerabilities/230710150218060/

Краткое описание: Выполнение произвольного кода в SonicWall GMS и Analytics

Идентификатор уязвимости: CVE-2023-34133

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

Уязвимый продукт: SonicWall GMS и Analytics:
SonicWall GMS: 9.3.2-SP1 - 9.3.2-SP1
SonicWall Analytics: 2.5.0.4-R7 - 2.5.0.4-R7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

35

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0010
- http://www.sonicwall.com/support/knowledge-base/urgent-security-notice-sonicwall-gms-analytics-impacted-by-suite-of-vulnerabilities/230710150218060/

Краткое описание: Выполнение произвольного кода в SonicWall GMS и Analytics

Идентификатор уязвимости: CVE-2023-34127

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

Уязвимый продукт: SonicWall GMS и Analytics:
SonicWall GMS: 9.3.2-SP1 - 9.3.2-SP1
SonicWall Analytics: 2.5.0.4-R7 - 2.5.0.4-R7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

36

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0010
- http://www.sonicwall.com/support/knowledge-base/urgent-security-notice-sonicwall-gms-analytics-impacted-by-suite-of-vulnerabilities/230710150218060/

Краткое описание: Выполнение произвольного кода в SonicWall GMS и Analytics

Идентификатор уязвимости: CVE-2023-34124

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: SonicWall GMS и Analytics:
SonicWall GMS: 9.3.2-SP1 - 9.3.2-SP1
SonicWall Analytics: 2.5.0.4-R7 - 2.5.0.4-R7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0010
- http://www.sonicwall.com/support/knowledge-base/urgent-security-notice-sonicwall-gms-analytics-impacted-by-suite-of-vulnerabilities/230710150218060/

38

Краткое описание: Обход безопасности в GeoVision GV-ADR2701

Идентификатор уязвимости: CVE-2023-3638

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: GeoVision GV-ADR2701: 1.00_2017_12_15 - 1.00_2017_12_15

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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: 2023-07-19 / 2023-07-19

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-199-05

Краткое описание: Повышение привилегий в WordPress-плагин WooCommerce Payments

Идентификатор уязвимости: CVE-2023-28121

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: WordPress-плагин WooCommerce Payments: 4.8.0 - 4.8.2.

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

39 **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: 2023-07-03 / 2023-07-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-28121

Краткое описание: Выполнение произвольного кода в Citrix ADC и Citrix Gateway

Идентификатор уязвимости: CVE-2023-3519

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

Уязвимый продукт: Citrix ADC и Citrix Gateway:
NetScaler ADC и NetScaler Gateway до 13.1–49.13
NetScaler ADC и NetScaler Gateway до 13.0–91.13
NetScaler ADC до 13.1-FIPS 13.1-37.159
NetScaler ADC до 12.1-FIPS 12.1-55.297
NetScaler ADC до 12.1-NDcPP 12.1-55.297

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

40

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: 2023-07-18 / 2023-07-18

Ссылки на источник:

- https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

Краткое описание: Повышение привилегий в Citrix ADC и Citrix Gateway

Идентификатор уязвимости: CVE-2023-3467

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Citrix ADC и Citrix Gateway:
NetScaler ADC и NetScaler Gateway до 13.1–49.13
NetScaler ADC и NetScaler Gateway до 13.0–91.13
NetScaler ADC до 13.1-FIPS 13.1-37.159
NetScaler ADC до 12.1-FIPS 12.1-55.297
NetScaler ADC до 12.1-NDcPP 12.1-55.297

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

41

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/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: 2023-07-18 / 2023-07-18

Ссылки на источник:

- https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

Краткое описание: Межсайтовый скриптинг в Citrix ADC и Citrix Gateway

Идентификатор уязвимости: CVE-2023-3466

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Citrix ADC и Citrix Gateway:
NetScaler ADC и NetScaler Gateway до 13.1–49.13
NetScaler ADC и NetScaler Gateway до 13.0–91.13
NetScaler ADC до 13.1-FIPS 13.1-37.159
NetScaler ADC до 12.1-FIPS 12.1-55.297
NetScaler ADC до 12.1-NDcPP 12.1-55.297

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

42

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-18 / 2023-07-18

Ссылки на источник:

- https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

Краткое описание: Выполнение произвольного кода в Zyxel firewalls and WLAN controllers

Идентификатор уязвимости: CVE-2023-34141

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

Уязвимый продукт: Zyxel firewalls and WLAN controllers:
ATP series: 5.00 - 5.36 Patch 2
USG FLEX series: 5.00 - 5.36 Patch 2
USG FLEX 50W: 5.00 - 5.36 Patch 2
USG20W-VPN: 5.00 - 5.36 Patch 2
VPN series: 5.00 - 5.36 Patch 2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

43 **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: 8.0 AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers

Краткое описание: Выполнение произвольного кода в Zyxel firewalls and WLAN controllers

Идентификатор уязвимости: CVE-2023-34139

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

Уязвимый продукт: Zyxel firewalls and WLAN controllers:
USG FLEX series: 4.50 - 5.36 Patch 2
VPN series: 4.20 - 5.36 Patch 2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

44 **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: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: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers

Краткое описание: Выполнение произвольного кода в Zyxel firewalls and WLAN controllers

Идентификатор уязвимости: CVE-2023-34138

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

Уязвимый продукт: Zyxel firewalls and WLAN controllers:
ATP series: 4.60 - 5.36 Patch 2
USG FLEX series: 4.60 - 5.36 Patch 2
USG FLEX 50W: 4.60 - 5.36 Patch 2
USG20W-VPN: 4.60 - 5.36 Patch 2
VPN series: 4.60 - 5.36 Patch 2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

45 **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: 8.0 AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers

Краткое описание: Выполнение произвольного кода в Zyxel firewalls and WLAN controllers

Идентификатор уязвимости: CVE-2023-33012

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

Уязвимый продукт: Zyxel firewalls and WLAN controllers:
ATP series: 5.10 - 5.36 Patch 2
USG FLEX series: 5.00 - 5.36 Patch 2
USG FLEX 50W: 5.10 - 5.36 Patch 2
USG20W-VPN: 5.10 - 5.36 Patch 2
VPN series: 5.00 - 5.36 Patch 2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

46 **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: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: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers

47

Краткое описание: Выполнение произвольного кода в Zyxel firewalls and WLAN controllers

Идентификатор уязвимости: CVE-2023-33011

Идентификатор программной ошибки: CWE-134 Использование форматной строки, контролируемой извне

Уязвимый продукт: Zyxel firewalls and WLAN controllers:
ATP series: 5.10 - 5.36 Patch 2
USG FLEX series: 5.00 - 5.36 Patch 2
USG FLEX 50W: 5.10 - 5.36 Patch 2
USG20W-VPN: 5.10 - 5.36 Patch 2
VPN series: 5.00 - 5.36 Patch 2

Категория уязвимого продукта: Средства защиты информации

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: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: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers

Краткое описание: Выполнение произвольного кода в Zyxel firewalls and WLAN controllers

Идентификатор уязвимости: CVE-2023-28767

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

Уязвимый продукт: Zyxel firewalls and WLAN controllers:
ATP series: 5.10 - 5.36
USG FLEX series: 5.00 - 5.36
USG FLEX 50W: 5.10 - 5.36
USG20W-VPN: 5.10 - 5.36
VPN series: 5.00 - 5.36

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

48 **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: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: 2023-07-18 / 2023-07-18

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers