НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-09-06.1 | 6 сентября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-32257	Linux kernel	Сетевой	ACE	2023-09-06	✓
2	Критическая	CVE-2023-39240	ASUS Routers	Сетевой	ACE	2023-09-06	✓
3	Критическая	CVE-2023-39239	ASUS Routers	Сетевой	ACE	2023-09-06	✓
4	Критическая	CVE-2023-39238	ASUS Routers	Сетевой	ACE	2023-09-06	✓
5	Высокая	CVE-2023-39237	ASUS RT-AC86U	Сетевой	ACE	2023-09-06	✓
6	Высокая	CVE-2023-39236	ASUS RT-AC86U	Сетевой	ACE	2023-09-06	✓
7	Высокая	CVE-2023-38033	ASUS RT-AC86U	Сетевой	ACE	2023-09-06	✓
8	Высокая	CVE-2023-38032	ASUS RT-AC86U	Сетевой	ACE	2023-09-06	✓
9	Высокая	CVE-2023-38031	ASUS RT-AC86U	Сетевой	ACE	2023-09-06	✓

1

Краткое описание: Выполнение произвольного кода в Linux kernel

Идентификатор уязвимости: CVE-2023-32257

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: Linux kernel: все версии

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-06 / 2023-09-06

Ссылки на источник:

- http://bugzilla.redhat.com/show_bug.cgi?id=2219806
- http://github.com/torvalds/linux/commit/f5c779b7ddbda30866cf2a27c63e34158f858c73
- http://www.zerodayinitiative.com/advisories/ZDI-23-705/
- https://bdu.fstec.ru/vul/2023-02742

2

Краткое описание: Выполнение произвольного кода в ASUS Routers

Идентификатор уязвимости: CVE-2023-39240

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

Уязвимый продукт: ASUS Routers:
RT-AX55: 3.0.0.4.386_50460
RT-AX56U_V2: 3.0.0.4.386_50460
RT-AC86U: 3.0.0.4_386_51529

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

Дата выявления / Дата обновления: 2023-09-06 / 2023-09-06

Ссылки на источник:

- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230906
- http://www.twcert.org.tw/tw/cp-132-7356-021bf-1.html

3

Краткое описание: Выполнение произвольного кода в ASUS Routers

Идентификатор уязвимости: CVE-2023-39239

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

Уязвимый продукт: ASUS Routers:
RT-AX55: 3.0.0.4.386_50460
RT-AX56U_V2: 3.0.0.4.386_50460
RT-AC86U: 3.0.0.4_386_51529

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

Дата выявления / Дата обновления: 2023-09-06 / 2023-09-06

Ссылки на источник:

- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230906
- http://www.twcert.org.tw/tw/cp-132-7355-0ce8d-1.html

4

Краткое описание: Выполнение произвольного кода в ASUS Routers

Идентификатор уязвимости: CVE-2023-39238

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

Уязвимый продукт: ASUS Routers:
RT-AX55: 3.0.0.4.386_50460
RT-AX56U_V2: 3.0.0.4.386_50460
RT-AC86U: 3.0.0.4_386_51529

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

Дата выявления / Дата обновления: 2023-09-06 / 2023-09-06

Ссылки на источник:

- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230906
- http://www.twcert.org.tw/tw/cp-132-7354-4e654-1.html

Краткое описание: Выполнение произвольного кода в ASUS RT-AC86U

Идентификатор уязвимости: CVE-2023-39237

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

Уязвимый продукт: ASUS RT-AC86U: 3.0.0.4_386_51529

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-09-06 / 2023-09-06

Ссылки на источник:

- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230906
- http://www.twcert.org.tw/tw/cp-132-7352-bad68-1.html

6

Краткое описание: Выполнение произвольного кода в ASUS RT-AC86U

Идентификатор уязвимости: CVE-2023-39236

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

Уязвимый продукт: ASUS RT-AC86U: 3.0.0.4_386_51529

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

Дата выявления / Дата обновления: 2023-09-06 / 2023-09-06

Ссылки на источник:

- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230906
- http://www.twcert.org.tw/tw/cp-132-7351-ec8fe-1.html

Краткое описание: Выполнение произвольного кода в ASUS RT-AC86U

Идентификатор уязвимости: CVE-2023-38033

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

Уязвимый продукт: ASUS RT-AC86U: 3.0.0.4_386_51529

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

7 **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: 2023-09-06 / 2023-09-06

Ссылки на источник:

- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230906
- http://www.twcert.org.tw/tw/cp-132-7350-ded5e-1.html

8

Краткое описание: Выполнение произвольного кода в ASUS RT-AC86U

Идентификатор уязвимости: CVE-2023-38032

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

Уязвимый продукт: ASUS RT-AC86U: 3.0.0.4_386_51529

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

Дата выявления / Дата обновления: 2023-09-06 / 2023-09-06

Ссылки на источник:

- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230906
- http://www.twcert.org.tw/tw/cp-132-7349-7f8cd-1.html

Краткое описание: Выполнение произвольного кода в ASUS RT-AC86U

Идентификатор уязвимости: CVE-2023-38031

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

Уязвимый продукт: ASUS RT-AC86U: 3.0.0.4_386_51529

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

9 **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: 2023-09-06 / 2023-09-06

Ссылки на источник:

- http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230906
- http://www.twcert.org.tw/tw/cp-132-7348-56989-1.html