НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-05-31.1 | 31 мая 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-32763	Qt	Локальный	ACE	2023-05-30	✓
2	Высокая	CVE-2023-2610	Vim	Локальный	ACE	2023-05-30	✓
3	Критическая	CVE-2023-27407	Siemens SCALANCE LPE9403	Сетевой	ACE	2023-05-10	✓
4	Высокая	CVE-2023-22922	Zyxel NBG-418N v2	Сетевой	DoS	2023-05-02	✓
5	Высокая	CVE-2023-22921	Zyxel NBG-418N v2	Сетевой	XSS\CSS	2023-05-02	✓
6	Высокая	CVE-2023-22919	Zyxel NBG6604	Сетевой	ACE	2023-05-02	✓
7	Критическая	CVE-2023-25690	Zimbra Collaboration	Сетевой	SB	2023-05-30	✓
8	Высокая	CVE-2023-0286	HPE HP-UX OpenSSL	Сетевой	DoS	2023-05-30	✓
9	Высокая	CVE-2023-0215	HPE HP-UX OpenSSL	Сетевой	DoS	2023-05-30	✓
10	Высокая	CVE-2023-27988	Zyxel NAS products	Сетевой	ACE	2023-05-30	✓
11	Высокая	CVE-2023-0950	LibreOffice	Сетевой	ACE	2023-05-29	✓
12	Высокая	CVE-2023-32154	MikroTik RouterOS	Смежная сеть	ACE	2023-05-18	✓

1

Краткое описание: Выполнение произвольного кода в Qt

Идентификатор уязвимости: CVE-2023-32763

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

Уязвимый продукт: Qt: 5.15.0 - 6.5.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-05-30 / 2023-05-30

Ссылки на источник:

- http://lists.qt-project.org/pipermail/announce/2023-May/000413.html
- http://codereview.qt-project.org/c/qt/qtbase/+/476125

2

Краткое описание: Выполнение произвольного кода в Vim

Идентификатор уязвимости: CVE-2023-2610

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Vim: до 9.0.1532

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: 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: 2023-05-30 / 2023-05-30

Ссылки на источник:

- http://github.com/vim/vim/commit/ab9a2d884b3a4abe319606ea95a5a6d6b01cd73a
- http://huntr.dev/bounties/31e67340-935b-4f6c-a923-f7246bc29c7d
- http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/PCLJN4QINITA3ZASKLEJ64C5TFNKELMO/

3

Краткое описание: Выполнение произвольного кода в Siemens SCALANCE LPE9403

Идентификатор уязвимости: CVE-2023-27407

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

Уязвимый продукт: Siemens SCALANCE LPE9403: до 2.1

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: 2023-05-10 / 2023-05-10

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-325383.pdf
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-131-06
- https://bdu.fstec.ru/vul/2023-02468

4

Краткое описание: Отказ в обслуживании в Zyxel NBG-418N v2

Идентификатор уязвимости: CVE-2023-22922

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

Уязвимый продукт: Zyxel NBG-418N v2: 1.00(AARP.13)C0 - 1.00(AARP.13)C0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV: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: 2023-05-02 / 2023-05-02

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nbg-418n-v2-home-router
- https://bdu.fstec.ru/vul/2023-02403

5

Краткое описание: Межсайтовый скриптинг в Zyxel NBG-418N v2

Идентификатор уязвимости: CVE-2023-22921

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

Уязвимый продукт: Zyxel NBG-418N v2: 1.00(AARP.13)C0 - 1.00(AARP.13)C0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-02 / 2023-05-02

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nbg-418n-v2-home-router
- https://bdu.fstec.ru/vul/2023-02378

6

Краткое описание: Выполнение произвольного кода в Zyxel NBG6604

Идентификатор уязвимости: CVE-2023-22919

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

Уязвимый продукт: Zyxel NBG6604: 1.01(ABIR.0)C0 - 1.01(ABIR.0)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: 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: 2023-05-02 / 2023-05-02

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerability-in-nbg6604-home-router
- https://bdu.fstec.ru/vul/2023-02404

7

Краткое описание: Обход безопасности в Zimbra Collaboration

Идентификатор уязвимости: CVE-2023-25690

Идентификатор программной ошибки: CWE-113 Некорректная нейтрализация последовательностей символов CRLF в HTTP-заголовках (расщепление HTTP-ответов)

Уязвимый продукт: Zimbra Collaboration: 8.8 - 10.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2023-05-30 / 2023-05-30

Ссылки на источник:

- http://wiki.zimbra.com/wiki/Security_Center#ZCS_8.8.15_Patch_40_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_9.0.0_Patch_33_Released
- https://bdu.fstec.ru/vul/2023-01738

8

Краткое описание: Отказ в обслуживании в HPE HP-UX OpenSSL

Идентификатор уязвимости: CVE-2023-0286

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: HPE HP-UX OpenSSL: до A.01.01.01t.001

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.4 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-30 / 2023-05-30

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04475en_us
- https://bdu.fstec.ru/vul/2023-00665

9

Краткое описание: Отказ в обслуживании в HPE HP-UX OpenSSL

Идентификатор уязвимости: CVE-2023-0215

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: HPE HP-UX OpenSSL: до A.01.01.01t.001

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2023-05-30 / 2023-05-30

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04475en_us
- https://bdu.fstec.ru/vul/2023-00675

10

Краткое описание: Выполнение произвольного кода в Zyxel NAS products

Идентификатор уязвимости: CVE-2023-27988

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.12)C0 - 5.21(AAZF.12)C0
NAS540: 5.21(AATB.9)C0 - 5.21(AATB.9)C0
NAS542: 5.21(ABAG.9)C0 - 5.21(ABAG.9)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: 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: 2023-05-30 / 2023-05-30

Ссылки на источник:

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

Краткое описание: Выполнение произвольного кода в LibreOffice

Идентификатор уязвимости: CVE-2023-0950

Идентификатор программной ошибки: CWE-129 Некорректная проверка индекса массива

Уязвимый продукт: LibreOffice: 7.4.0.1 - 7.5.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

11 **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:L/PR:N/UI:R/S:U/C:L/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-29 / 2023-05-29

Ссылки на источник:

- http://www.libreoffice.org/about-us/security/advisories/CVE-2023-0950

12

Краткое описание: Выполнение произвольного кода в MikroTik RouterOS

Идентификатор уязвимости: CVE-2023-32154

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: MikroTik RouterOS: 6.0 - 7.9

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: 7.5 AV:A/AC:H/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: 2023-05-18 / 2023-05-23

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-23-710/
- https://bdu.fstec.ru/vul/2023-02827