НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-12-01.1 | 1 декабря 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-47039	cPanel EasyApache	Локальный	PE	2023-12-01	✓
2	Критическая	CVE-2023-47038	cPanel EasyApache	Сетевой	ACE	2023-12-01	✓
3	Не определено	CVE-2023-42917	Apple macOS Sonoma и Apple Safari	Не определено	ACE	2023-12-01	✓
4	Не определено	CVE-2023-42916	Apple macOS Sonoma и Apple Safari	Не определено	ACE	2023-12-01	✓
5	Не определено	CVE-2023-42916	WebKitGTK+ и WPE WebKit	Не определено	ACE	2023-12-01	✗
6	Не определено	CVE-2023-42917	WebKitGTK+ и WPE WebKit	Не определено	ACE	2023-12-01	✗
7	Высокая	CVE-2023-6360	My Calendar плагин WordPress	Сетевой	ACE	2023-11-30	✓
8	Критическая	CVE-2023-48365	Qlik Sense Enterprise for Windows	Сетевой	PE	2023-11-30	✓
9	Критическая	CVE-2023-4474	Zyxel NAS products	Сетевой	ACE	2023-11-30	✓
10	Критическая	CVE-2023-4473	Zyxel NAS products	Сетевой	ACE	2023-11-30	✓
11	Высокая	CVE-2023-37928	Zyxel NAS products	Сетевой	ACE	2023-11-30	✓
12	Высокая	CVE-2023-37927	Zyxel NAS products	Сетевой	ACE	2023-11-30	✓

13	Критическая	CVE-2023-35138	Zyxel NAS products	Сетевой	ACE	2023-11-30	✓
14	Высокая	CVE-2023-35137	Zyxel NAS products	Сетевой	SB	2023-11-30	✓

1

Краткое описание: Повышение привилегий в cPanel EasyApache

Идентификатор уязвимости: CVE-2023-47039

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: cPanel EasyApache: до 4 2023-11-30

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 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

Дата выявления / Дата обновления: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://news.cpanel.com/easyapache4-2023-11-30-maintenance-and-security-release/
- https://bdu.fstec.ru/vul/2023-08230

2

Краткое описание: Выполнение произвольного кода в cPanel EasyApache

Идентификатор уязвимости: CVE-2023-47038

Идентификатор программной ошибки: CWE-193 Ошибка смещения на единицу

Уязвимый продукт: cPanel EasyApache: до 4 2023-11-30

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://news.cpanel.com/easyapache4-2023-11-30-maintenance-and-security-release/
- https://bdu.fstec.ru/vul/2023-08229

3

Краткое описание: Выполнение произвольного кода в Apple macOS Sonoma и Apple Safari

Идентификатор уязвимости: CVE-2023-42917

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

Уязвимый продукт: Apple macOS Sonoma и Apple Safari:

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: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Дата выявления / Дата обновления: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://support.apple.com/en-us/HT214033
- http://support.apple.com/en-us/HT214032

Краткое описание: Выполнение произвольного кода в Apple macOS Sonoma и Apple Safari

Идентификатор уязвимости: CVE-2023-42916

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Apple macOS Sonoma и Apple Safari:
Apple Safari: 17.0 - 17.1
macOS: 14.0 23A344 - 14.1 23B74

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

4

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: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Дата выявления / Дата обновления: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://support.apple.com/en-us/HT214033
- http://support.apple.com/en-us/HT214032

5

Краткое описание: Выполнение произвольного кода в WebKitGTK+ и WPE WebKit

Идентификатор уязвимости: CVE-2023-42916

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: WebKitGTK+ и WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Дата выявления / Дата обновления: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://support.apple.com/en-us/HT214033
- http://support.apple.com/en-us/HT214032
- http://support.apple.com/en-us/HT214031

6

Краткое описание: Выполнение произвольного кода в WebKitGTK+ и WPE WebKit

Идентификатор уязвимости: CVE-2023-42917

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

Уязвимый продукт: WebKitGTK+ и WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Дата выявления / Дата обновления: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://support.apple.com/en-us/HT214033
- http://support.apple.com/en-us/HT214032
- http://support.apple.com/en-us/HT214031

Краткое описание: Выполнение произвольного кода в My Calendar плагин WordPress

Идентификатор уязвимости: CVE-2023-6360

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

Уязвимый продукт: My Calendar плагин WordPress: 3.0.0 - 3.4.21

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-30 / 2023-11-30

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2023-40
- http://www.joedolson.com/2023/11/my-calendar-3-4-22-security-release/

8

Краткое описание: Повышение привилегий в Qlik Sense Enterprise for Windows

Идентификатор уязвимости: CVE-2023-48365

Идентификатор программной ошибки: CWE-444 Некорректная интерпретация HTTP-запросов (несанкционированные HTTP-запросы)

Уязвимый продукт: Qlik Sense Enterprise for Windows: до November 2022 Patch 12

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Туннелирование HTTP-запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-30 / 2023-11-30

Ссылки на источник:

- http://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510

9

Краткое описание: Выполнение произвольного кода в Zyxel NAS products

Идентификатор уязвимости: CVE-2023-4474

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: Zyxel NAS products:
NAS326: 5.21(AAZF.14)C0
NAS542: 5.21(ABAG.11)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

Дата выявления / Дата обновления: 2023-11-30 / 2023-11-30

Ссылки на источник:

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

10

Краткое описание: Выполнение произвольного кода в Zyxel NAS products

Идентификатор уязвимости: CVE-2023-4473

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.14)C0
NAS542: 5.21(ABAG.11)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

Дата выявления / Дата обновления: 2023-11-30 / 2023-11-30

Ссылки на источник:

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

11

Краткое описание: Выполнение произвольного кода в Zyxel NAS products

Идентификатор уязвимости: CVE-2023-37928

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.14)C0
NAS542: 5.21(ABAG.11)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

Дата выявления / Дата обновления: 2023-11-30 / 2023-11-30

Ссылки на источник:

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

12

Краткое описание: Выполнение произвольного кода в Zyxel NAS products

Идентификатор уязвимости: CVE-2023-37927

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: Zyxel NAS products:
NAS326: 5.21(AAZF.14)C0
NAS542: 5.21(ABAG.11)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

Дата выявления / Дата обновления: 2023-11-30 / 2023-11-30

Ссылки на источник:

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

13

Краткое описание: Выполнение произвольного кода в Zyxel NAS products

Идентификатор уязвимости: CVE-2023-35138

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.14)C0
NAS542: 5.21(ABAG.11)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

Дата выявления / Дата обновления: 2023-11-30 / 2023-11-30

Ссылки на источник:

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

Краткое описание: Обход безопасности в Zyxel NAS products

Идентификатор уязвимости: CVE-2023-35137

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Zyxel NAS products:
NAS326: 5.21(AAZF.14)C0
NAS542: 5.21(ABAG.11)C0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: обход безопасности

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-30 / 2023-11-30

Ссылки на источник:

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