НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-09-11.1 | 11 сентября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-40397	WebKitG	Сетевой	ACE	2023-09-11	✗
2	Высокая	CVE-2023-42038	Kofax PowerPDF Advanced	Локальный	ACE	2023-09-11	✓
3	Высокая	CVE-2023-42036	Kofax PowerPDF Advanced	Локальный	ACE	2023-09-11	✓
4	Высокая	CVE-2023-42037	Kofax PowerPDF Advanced	Локальный	ACE	2023-09-11	✓
5	Высокая	CVE-2023-42039	Kofax PowerPDF Advanced	Локальный	ACE	2023-09-11	✓
6	Высокая	CVE-2023-40031	Notepad++	Локальный	ACE	2023-09-08	✓
7	Средняя	CVE-2023-20269	Cisco Adaptive Security Appliance (ASA)	Сетевой	SB	2023-09-07	✓
8	Высокая	CVE-2023-4763	Microsoft Edge	Сетевой	ACE	2023-09-07	✓
9	Высокая	CVE-2023-4762	Microsoft Edge	Сетевой	ACE	2023-09-07	✓
10	Высокая	CVE-2023-4761	Microsoft Edge	Сетевой	ACE	2023-09-07	✓
11	Критическая	CVE-2023-41064	Apple macOS Ventura	Сетевой	ACE	2023-09-07	✓
12	Критическая	CVE-2023-20238	Cisco BroadWorks Application Delivery Platform and Xtended Services Platform	Сетевой	SB	2023-09-07	✓
13	Высокая	CVE-2023-20243	Cisco Identity Services Engine (ISE)	Сетевой	DoS	2023-09-07	✓

1

Краткое описание: Выполнение произвольного кода в WebKitG

Идентификатор уязвимости: CVE-2023-40397

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

Уязвимый продукт: WebKitG:
WebKitGTK+: все версии
WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-11 / 2023-09-11

Ссылки на источник:

- http://support.apple.com/en-us/HT213843

2

Краткое описание: Выполнение произвольного кода в Kofax PowerPDF Advanced

Идентификатор уязвимости: CVE-2023-42038

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Kofax PowerPDF Advanced: до 5.0.0.12

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

Дата выявления / Дата обновления: 2023-09-11 / 2023-09-11

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1394/
- http://docshield.kofax.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.12.htm

3

Краткое описание: Выполнение произвольного кода в Kofax PowerPDF Advanced

Идентификатор уязвимости: CVE-2023-42036

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

Уязвимый продукт: Kofax PowerPDF Advanced: до 5.0.0.12

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

Дата выявления / Дата обновления: 2023-09-11 / 2023-09-11

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1393/
- http://docshield.kofax.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.12.htm

4

Краткое описание: Выполнение произвольного кода в Kofax PowerPDF Advanced

Идентификатор уязвимости: CVE-2023-42037

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

Уязвимый продукт: Kofax PowerPDF Advanced: до 5.0.0.12

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

Дата выявления / Дата обновления: 2023-09-11 / 2023-09-11

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1392/
- http://docshield.kofax.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.12.htm

5

Краткое описание: Выполнение произвольного кода в Kofax PowerPDF Advanced

Идентификатор уязвимости: CVE-2023-42039

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Kofax PowerPDF Advanced: до 5.0.0.12

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

Дата выявления / Дата обновления: 2023-09-11 / 2023-09-11

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1395/
- http://docshield.kofax.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.12.htm

Краткое описание: Выполнение произвольного кода в Notepad++

Идентификатор уязвимости: CVE-2023-40031

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Notepad++: 8.1 - 8.5.6

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.

6

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

Дата выявления / Дата обновления: 2023-09-08 / 2023-09-08

Ссылки на источник:

- http://github.com/notepad-plus-plus/notepad-plus-plus/releases/tag/v8.5.7
- http://securitylab.github.com/advisories/GHSL-2023-092_Notepad__/
- http://github.com/notepad-plus-plus/notepad-plus-plus/issues/14073
- http://notepad-plus-plus.org/news/v857-released-fix-security-issues/
- https://bdu.fstec.ru/vul/2023-05051

Краткое описание: Обход безопасности в Cisco Adaptive Security Appliance (ASA)

Идентификатор уязвимости: CVE-2023-20269

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: Cisco Adaptive Security Appliance (ASA): 6.2.3 - 9.19.1.18
Cisco Firepower Threat Defense (FTD): 6.2.3 - 9.19.1.18

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-07 / 2023-09-07

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

8

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-4763

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 116.0.1938.69

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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

Дата выявления / Дата обновления: 2023-09-07 / 2023-09-07

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-4763
- https://bdu.fstec.ru/vul/2023-05249

9

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-4762

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 116.0.1938.69

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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

Дата выявления / Дата обновления: 2023-09-07 / 2023-09-07

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-4762
- https://bdu.fstec.ru/vul/2023-05240

10

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-4761

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 116.0.1938.69

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-07 / 2023-09-07

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-4761
- https://bdu.fstec.ru/vul/2023-05241

Краткое описание: Выполнение произвольного кода в Apple macOS Ventura

Идентификатор уязвимости: CVE-2023-41064

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

Уязвимый продукт: Apple macOS Ventura: 13.0 22A380 - 13.5.1 22G90

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

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: 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: 2023-09-07 / 2023-09-07

Ссылки на источник:

- http://support.apple.com/en-us/HT213906

Краткое описание: Обход безопасности в Cisco BroadWorks Application Delivery Platform and Xtended Services Platform

Идентификатор уязвимости: CVE-2023-20238

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Cisco BroadWorks Application Delivery Platform and Xtended Services Platform:
BroadWorks Application Delivery Platform: 22.0 - 23.0
BroadWorks Xtended Services Platform: 22.0 - 23.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

12

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

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-07 / 2023-09-07

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-auth-bypass-kCggMWhX
- https://bdu.fstec.ru/vul/2023-05316

13

Краткое описание: Отказ в обслуживании в Cisco Identity Services Engine (ISE)

Идентификатор уязвимости: CVE-2023-20243

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Cisco Identity Services Engine (ISE): 3.1 - 3.2

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-07 / 2023-09-07

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radius-dos-W7cNn7gt
- https://bdu.fstec.ru/vul/2023-05366