НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-09-04.1 | 4 сентября 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-39689	Certifi python-certifi	Сетевой	ACE	2024-09-03	✓
2	Высокая	CVE-2024-5412	Zyxel products	Сетевой	DoS	2024-09-03	✓
3	Высокая	CVE-2024-42058	Zyxel firewalls	Сетевой	DoS	2024-09-03	✓
4	Высокая	CVE-2024-42057	Zyxel firewalls	Сетевой	ACE	2024-09-03	✓
5	Критическая	CVE-2024-22442	HPE 3PAR Service Processor	Сетевой	SB	2024-09-03	✓
6	Критическая	CVE-2024-7261	Zyxel APs and security router devices	Сетевой	ACE	2024-09-03	✓
7	Высокая	CVE-2024-5461	HPE Brocade Fabric OS	Смежная сеть	ACE	2024-09-03	✓
8	Критическая	CVE-2024-7970	Google Chrome	Сетевой	ACE	2024-09-02	✓
9	Критическая	CVE-2024-8362	Google Chrome	Сетевой	ACE	2024-09-02	✓
10	Критическая	CVE-2024-2961	Traffix SDC OpenSSL component	Сетевой	ACE	2024-09-02	✗
11	Высокая	CVE-2024-7013	Panasonic Control FPWIN Pro	Локальный	ACE	2024-08-30	✓
12	Высокая	CVE-2024-7971	Google ChromeOS	Сетевой	ACE	2024-08-30	✓
13	Высокая	CVE-2024-20446	Cisco NX-OS Software	Сетевой	DoS	2024-08-29	✓

14	Высокая	CVE-2024-8198	Google Chrome	Сетевой	ACE	2024-08-28	✓
15	Высокая	CVE-2024-8194	Google Chrome	Сетевой	ACE	2024-08-28	✓
16	Высокая	CVE-2024-8193	Google Chrome	Сетевой	ACE	2024-08-28	✓
17	Высокая	CVE-2024-7969	Google Chrome	Сетевой	ACE	2024-08-28	✓
18	Высокая	CVE-2024-7263	Kingsoft WPS Office	Локальный	ACE	2024-08-28	✓
19	Высокая	CVE-2024-7262	Kingsoft WPS Office	Локальный	ACE	2024-08-28	✓
20	Критическая	CVE-2024-6633	Fortra FileCatalyst Workflow	Сетевой	PE	2024-08-28	✓
21	Высокая	CVE-2024-43689	ELECOM wireless LAN routers and access points	Смежная сеть	ACE	2024-08-27	✓
22	Высокая	CVE-2024-39300	ELECOM wireless LAN routers and access points	Сетевой	OSI	2024-08-27	✓

1

Краткое описание: Выполнение произвольного кода в Certifi python-certifi

Идентификатор уязвимости: CVE-2024-39689

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: python-certifi: 2022.05.18 - 2024.07.04

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:N/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-03 / 2024-09-03

Ссылки на источник:

- http://github.com/certifi/python-certifi/security/advisories/GHSA-248v-346w-9cwc
- http://github.com/certifi/python-certifi/commit/bd8153872e9c6fc98f4023df9c2deaffea2fa463
- http://groups.google.com/a/mozilla.org/g/dev-security-policy/c/XpknYMPO8dI

2

Краткое описание: Отказ в обслуживании в Zyxel products

Идентификатор уязвимости: CVE-2024-5412

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

Уязвимый продукт: NR5103: 4.19(ABYC.5)C0
NR5103Ev2: 1.00 ACIQ.0C0
NR5307: 1.00(ACJT.0)B5
NR7103: 1.00(ACCZ.3)C0
NR7302: 1.00(ACHA.3)C0
NR7303: 1.00(ACEI.1)B3
NR7501: 1.00(ACEH.1)B2
Nebula FWA510: 1.18(ACGC.2)C0
Nebula FWA710: 1.18(ACGC.2)C0
Nebula FWA505: 1.18(ACKO.2)C0
Nebula LTE3301-PLUS: 1.18(ACCA.2)C0
DX3300-T0: 5.50(ABVY.5)C0
DX3300-T1: 5.50(ABVY.5)C0
DX3301-T0: 5.50(ABVY.5)C0
DX4510-B0: 5.17(ABYL.6)C0
DX5401-B0: 5.17(ABYO.6)C0
DX5401-B1: 5.17(ABYO.6)C0
EX3300-T0: 5.50(ABVY.5)C0
EX3300-T1: 5.50(ABVY.5)C0
EX3301-T0: 5.50(ABVY.5)C0
EX3500-T0: 5.44(ACHR.1)C0
EX3501-T0: 5.44(ACHR.1)C0
EX3510-B0: 5.17(ABUP.11)C0
EX5401-B0: 5.17(ABYO.6)C0
EX5401-B1: 5.17(ABYO.6)C0
EX5510-B0: 5.17(ABQX.9)C0
EX5512-T0: 5.70(ACEG.3)C1
EX5601-T0: 5.70(ACDZ.3)C0
EX5601-T1: 5.70(ACDZ.3)C0
EX7501-B0: 5.18(ACHN.1)C0

EX7710-B0: 5.18(ACAK.1)C0
EMG3525-T50B: 5.50(ABPM.9)C0
EMG5523-T50B: 5.50(ABPM.9)C0
EMG5723-T50K: 5.50(ABOM.8)C0
VMG3625-T50B: 5.50(ABPM.9)C0
VMG3927-T50K: 5.50(ABOM.8)C0
VMG4005-B50A: 5.15(ABQA.2)C0
VMG4005-B60A: 5.15(ABQA.2)C0
VMG8623-T50B: 5.50(ABPM.9)C0
VMG8825-T50K: 5.50(ABOM.8)C0
AX7501-B0: 5.17(ABPC.5)C0
AX7501-B1: 5.17(ABPC.5)C0
PM3100-T0: 5.42(ACBF.2)C0
PM5100-T0: 5.42(ACBF.2)C0
PM7300-T0: 5.42(ABYY.2.1)C0
PX3321-T1: 5.44(ACJB.0)Z0
SCR50AXE: 1.10(ACGN.2)C0
WX3100-T0: 5.50(ABVL.4.1)C0
WX3401-B0: 5.17(ABVE.2.4)C0
WX5600-T0: 5.70(ACEB.3)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

Дата выявления / Дата обновления: 2024-09-03 / 2024-09-03

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024

Краткое описание: Отказ в обслуживании в Zyxel firewalls

Идентификатор уязвимости: CVE-2024-42058

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: ATP series: 4.32 - 5.38
USG FLEX series: 4.50 - 5.38
USG FLEX 50W: 4.20 - 5.38
USG20W-VPN: 4.20 - 5.38

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

3 **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

Дата выявления / Дата обновления: 2024-09-03 / 2024-09-03

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024

4

Краткое описание: Выполнение произвольного кода в Zyxel firewalls

Идентификатор уязвимости: CVE-2024-42057

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

Уязвимый продукт: ATP series: 4.32 - 5.38
USG FLEX series: 4.50 - 5.38
USG FLEX 50W: 4.16 - 5.38
USG20W-VPN: 4.16 - 5.38

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: 8.1 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: 2024-09-03 / 2024-09-03

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024

5

Краткое описание: Обход безопасности в HPE 3PAR Service Processor

Идентификатор уязвимости: CVE-2024-22442

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: 3PAR Service Processors: до 5.1.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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

Дата выявления / Дата обновления: 2024-09-03 / 2024-09-03

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04663en_us&docLocale=en_US

6

Краткое описание: Выполнение произвольного кода в Zyxel APs and security router devices

Идентификатор уязвимости: CVE-2024-7261

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

Уязвимый продукт: NWA50AX: 7.00(ABYW.1)
NWA50AX PRO: 7.00(ACGE.1)
NWA55AXE: 7.00(ABZL.1)
NWA90AX: 7.00(ACCV.1)
NWA90AX PRO: 7.00(ACGF.1)
NWA110AX: 7.00(ABTG.1)
NWA130BE: 7.00(ACIL.1)
NWA210AX: 7.00(ABTD.1)
NWA220AX-6E: 7.00(ACCO.1)
NWA1123-AC PRO: 6.28(ABHD.0)
NWA1123ACv3: 6.70(ABVT.4)
WAC500: 6.70(ABVS.4)
WAC500H: 6.70(ABWA.4)
WAC6103D-I: 6.28(AAXH.0)
WAC6502D-S: 6.28(AASE.0)
WAC6503D-S: 6.28(AASF.0)
WAC6552D-S: 6.28(ABIO.0)
WAC6553D-E: 6.28(AASG.2)
WAX300H: 7.00(ACHF.1)
WAX510D: 7.00(ABTF.1)
WAX610D: 7.00(ABTE.1)
WAX620D-6E: 7.00(ACCN.1)
WAX630S: 7.00(ABZD.1)
WAX640S-6E: 7.00(ACCM.1)
WAX650S: 7.00(ABRM.1)
WAX655E: 7.00(ACDO.1)
WBE530: 7.00(ACLE.1)

WBE660S: 7.00(ACGG.1)
USG LITE 60AX: 2.00(ACIP.2)

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: 2024-09-03 / 2024-09-03

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024

7

Краткое описание: Выполнение произвольного кода в HPE Brocade Fabric OS

Идентификатор уязвимости: CVE-2024-5461

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: HPE B-series SN6750B Fibre Channel Switch: все версии
HPE B-series SN6700B Fibre Channel Switch: все версии
HPE B-series SN6650B Fibre Channel Switch: все версии
HPE B-series SN6600B Fibre Channel Switch: все версии
HPE B-series SN4700B SAN Extension Switch: все версии
HPE B-series SN3600B Fibre Channel Switch: все версии
HPE B-series SN2600B SAN Extension Switch: все версии
HPE SN8600B 8-slot SAN Director Switch: все версии
HPE SN8600B 4-slot SAN Director Switch: все версии
HPE SN8700B 8-slot SAN Director Switch: все версии
HPE SN8700B 4-slot SAN Director Switch: все версии
Brocade 32Gb Fibre Channel SAN Switch for HPE Synergy: все версии
Brocade Fabric OS: до 9.2.1

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-03 / 2024-09-03

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04679en_us

8

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7970

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.114

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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-02 / 2024-09-02

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop.html
- http://crbug.com/358485426

9

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-8362

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.114

Категория уязвимого продукта: Прикладное программное обеспечение

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: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-02 / 2024-09-02

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop.html
- http://crbug.com/357391257

Краткое описание: Выполнение произвольного кода в Traffix SDC OpenSSL component

Идентификатор уязвимости: CVE-2024-2961
BDU:2024-03171

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

Уязвимый продукт: Traffix SDC: 5.1.0 - 5.2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

10 **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/E:P/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-02 / 2024-09-02

Ссылки на источник:

- http://my.f5.com/manage/s/article/K000140882
- https://bdu.fstec.ru/vul/2024-03171

11

Краткое описание: Выполнение произвольного кода в Panasonic Control FPWIN Pro

Идентификатор уязвимости: CVE-2024-7013

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Control FPWIN Pro: 7.7.2.0

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: 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: 2024-08-30 / 2024-08-30

Ссылки на источник:

- http://industry.panasonic.eu/products/automation-devices-solutions/programmable-logic-controllers-plc/plc-software/programming-software-control-fpwin-pro
- http://industry.panasonic.com/jp/ja/products/fasys/plc/software/fpwinpro7
- http://jvn.jp/en/vu/JVNVU99905584/index.html

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-7971
BDU:2024-06562

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

Уязвимый продукт: Chrome OS: до 126.0.6478.251

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

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

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-08-30 / 2024-08-30

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/long-term-support-channel-update-for_29.html
- https://bdu.fstec.ru/vul/2024-06562

Краткое описание: Отказ в обслуживании в Cisco NX-OS Software

Идентификатор уязвимости: CVE-2024-20446
BDU:2024-06551

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Cisco NX-OS: 8.2(11) - 10.2(1q)
Cisco Nexus 3000 Series Switches: все версии
Cisco Nexus 9000 Series Switches: все версии
Cisco Nexus 9000 Series Switches NX-OS Mode: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

13 **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: 2024-08-29 / 2024-08-29

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dhcp6-relay-dos-znEAA6xn
- https://bdu.fstec.ru/vul/2024-06551

14

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-8198

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.85

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

Дата выявления / Дата обновления: 2024-08-28 / 2024-08-28

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_28.html
- http://crbug.com/360758697

15

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-8194

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.85

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-08-28 / 2024-08-28

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_28.html
- http://crbug.com/360533914

16

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-8193

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.85

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

Дата выявления / Дата обновления: 2024-08-28 / 2024-08-28

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_28.html
- http://crbug.com/360265320

17

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7969

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.85

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-08-28 / 2024-08-28

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_28.html
- http://crbug.com/351865302

18

Краткое описание: Выполнение произвольного кода в Kingsoft WPS Office

Идентификатор уязвимости: CVE-2024-7263

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: WPS Office: 12.2.0.13110 - 12.2.0.16909

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: 2024-08-28 / 2024-08-28

Ссылки на источник:

- http://www.wps.com/whatsnew/pc/20240422/
- http://www.welivesecurity.com/en/eset-research/analysis-of-two-arbitrary-code-execution-vulnerabilities-affecting-wps-office/

19

Краткое описание: Выполнение произвольного кода в Kingsoft WPS Office

Идентификатор уязвимости: CVE-2024-7262

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: WPS Office: 12.2.0.13110 - 12.2.0.13306

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: 2024-08-28 / 2024-08-28

Ссылки на источник:

- http://www.wps.com/whatsnew/pc/20240422/
- http://www.welivesecurity.com/en/eset-research/analysis-of-two-arbitrary-code-execution-vulnerabilities-affecting-wps-office/

Краткое описание: Повышение привилегий в Fortra FileCatalyst Workflow

Идентификатор уязвимости: CVE-2024-6633

Идентификатор программной ошибки: CWE-276 Некорректные разрешения, назначаемые по умолчанию

Уязвимый продукт: FileCatalyst Workflow: до 5.1.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

Дата выявления / Дата обновления: 2024-08-28 / 2024-08-28

Ссылки на источник:

- http://www.fortra.com/security/advisories/product-security/fi-2024-011

Краткое описание: Выполнение произвольного кода в ELECOM wireless LAN routers and access points

Идентификатор уязвимости: CVE-2024-43689

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: WAB-I1750-PS: 1.5.10
WAB-S1167-PS: 1.5.6

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

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: 8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-27 / 2024-08-27

Ссылки на источник:

- http://jvn.jp/en/jp/JVN24885537/index.html
- http://www.elecom.co.jp/news/security/20240827-01/

22

Краткое описание: Получение конфиденциальной информации в ELECOM wireless LAN routers and access points

Идентификатор уязвимости: CVE-2024-39300

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: WAB-I1750-PS: 1.5.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-27 / 2024-08-27

Ссылки на источник:

- http://jvn.jp/en/jp/JVN24885537/index.html
- http://www.elecom.co.jp/news/security/20240827-01/