

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](https://cert.gov.ru)

E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

## Бюллетень об уязвимостях программного обеспечения

VULN.2024-09-30.1 | 30 сентября 2024 года

TLP: WHITE



## Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-47295	SEIKO EPSON Web Config	Сетевой	OSI	2024-09-30	✓
2	Высокая	CVE-2024-20350	Cisco DNA Center	Сетевой	OSI	2024-09-26	✓
3	Высокая	CVE-2024-20467	Cisco IOS XE Software IPv4 fragmentation reassembly	Сетевой	DoS	2024-09-25	✓
4	Высокая	CVE-2024-41708	AdaCore aws	Сетевой	OSI	2024-09-27	✗
5	Критическая	CVE-2024-8926	PHP	Сетевой	ACE	2024-09-27	✓
6	Критическая	CVE-2024-42507	HPE Aruba Networking Access Points	Сетевой	ACE	2024-09-26	✓
7	Критическая	CVE-2024-42506	HPE Aruba Networking Access Points	Сетевой	ACE	2024-09-26	✓
8	Критическая	CVE-2024-42505	HPE Aruba Networking Access Points	Сетевой	ACE	2024-09-26	✓
9	Критическая	CVE-2024-45492	Service Interconnect 1	Сетевой	ACE	2024-09-26	✓
10	Критическая	CVE-2024-45491	Service Interconnect 1	Сетевой	ACE	2024-09-26	✓
11	Критическая	CVE-2024-45490	Service Interconnect 1	Сетевой	ACE	2024-09-26	✓
12	Не определено	CVE-2024-6119	Service Interconnect 1	Не определено	DoS	2024-09-26	✓
13	Высокая	CVE-2024-6345	Service Interconnect 1	Сетевой	ACE	2024-09-26	✓

14	Высокая	CVE-2024-37370	Service Interconnect 1	Сетевой	SB	2024-09-26	✓
15	Критическая	CVE-2024-37371	Service Interconnect 1	Сетевой	OSI	2024-09-26	✓
16	Высокая	CVE-2024-20455	Cisco Catalyst SD-WAN Routers	Сетевой	DoS	2024-09-26	✓
17	Высокая	CVE-2024-20433	Cisco IOS and IOS XE Software	Сетевой	DoS	2024-09-26	✓
18	Высокая	CVE-2024-20436	Cisco IOS XE Software	Сетевой	DoS	2024-09-26	✓
19	Высокая	CVE-2024-20464	Cisco IOS XE Software	Сетевой	DoS	2024-09-26	✓
20	Высокая	CVE-2024-20480	Cisco IOS XE Software	Сетевой	DoS	2024-09-26	✓
21	Высокая	CVE-2024-39844	ZNC	Сетевой	ACE	2024-09-25	✓
22	Критическая	CVE-2024-8310	OPW Fuel Management Systems SiteSentinel	Сетевой	SB	2024-09-25	✓
23	Высокая	CVE-2024-6197	Nessus Network Monitor	Сетевой	ACE	2024-09-24	✓
24	Критическая	CVE-2024-45492	Nessus Network Monitor	Сетевой	ACE	2024-09-24	✓
25	Критическая	CVE-2024-45491	Nessus Network Monitor	Сетевой	ACE	2024-09-24	✓
26	Высокая	CVE-2024-6119	Nessus Network Monitor	Сетевой	DoS	2024-09-24	✓
27	Высокая	CVE-2024-9123	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-09-24	✓
28	Высокая	CVE-2024-9122	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-09-24	✓

29	Критическая	CVE-2024-9120	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-09-24	✓
30	Критическая	CVE-2024-46997	DataEase	Сетевой	ACE	2024-09-24	✓
31	Высокая	CVE-2024-46985	DataEase	Сетевой	OSI	2024-09-24	✓
32	Высокая	CVE-2024-9114	FastStone Image Viewer	Сетевой	ACE	2024-09-24	✗
33	Высокая	CVE-2024-9113	FastStone Image Viewer	Сетевой	ACE	2024-09-24	✗
34	Высокая	CVE-2024-9112	FastStone Image Viewer	Сетевой	ACE	2024-09-24	✗
35	Высокая	CVE-2024-8198	Google ChromeOS	Сетевой	ACE	2024-09-24	✓
36	Высокая	CVE-2024-8193	Google ChromeOS	Сетевой	ACE	2024-09-24	✓
37	Высокая	CVE-2024-7967	Google ChromeOS	Сетевой	ACE	2024-09-24	✓
38	Не определено	CVE-2024-8362	Google ChromeOS	Не определено	ACE	2024-09-24	✓
39	Высокая	CVE-2024-6989	Google ChromeOS	Сетевой	ACE	2024-09-24	✓
40	Высокая	CVE-2024-8805	BlueZ	Смежная сеть	ACE	2024-09-23	✓
41	Высокая	CVE-2024-7847	Rockwell Automation RSLogix 5 and RSLogix 500	Сетевой	ACE	2024-09-23	✗
42	Высокая	CVE-2023-45871	F5 Traffix SDC Linux kernel	Смежная сеть	ACE	2024-09-23	✗

**Краткое описание:** Получение конфиденциальной информации в SEIKO EPSON Web Config

**Идентификатор уязвимости:** CVE-2024-47295

**Идентификатор программной ошибки:** CWE-1188 Инициализация ресурса с небезопасными параметрами по умолчанию

**Уязвимый продукт:** Web Config: все версии

EP-10VA: все версии

EP-306: все версии

EP-30VA: все версии

EP-4004: все версии

EP-50V: все версии

EP-706A: все версии

EP-707A: все версии

EP-708A: все версии

EP-709A: все версии

EP-710A: все версии

EP-711A: все версии

EP-712A: все версии

EP-775A: все версии

EP-775AW: все версии

EP-776A: все версии

EP-777A: все версии

EP-802A: все версии

EP-803A: все версии

EP-803AW: все версии

EP-804A: все версии

EP-804AR: все версии

EP-804AW: все версии

EP-805A: все версии

EP-805AR: все версии

EP-805AW: все версии

EP-806AB: все версии

EP-806AR: все версии

EP-806AW: все версии

EP-807AB: все версии

EP-807AR: все версии  
EP-807AW: все версии  
EP-808AB: все версии  
EP-808AR: все версии  
EP-808AW: все версии  
EP-810AB: все версии  
EP-810AW: все версии  
EP-811AB: все версии  
EP-811AW: все версии  
EP-812A: все версии  
EP-879AB: все версии  
EP-879AR: все версии  
EP-879AW: все версии  
EP-880AB: все версии  
EP-880AN: все версии  
0AW: все версии  
EP-881AB: все версии  
EP-881AN: все версии  
EP-881AR: все версии  
EP-881AW: все версии  
EP-882AB: все версии  
EP-882AR: все версии  
EP-882AW: все версии  
EP-901A: все версии  
EP-901F: все версии  
EP-902A: все версии  
EP-903A: все версии  
EP-903F: все версии  
EP-904A: все версии  
EP-904F: все версии  
EP-905A: все версии  
EP-905F: все версии  
EP-906F: все версии  
EP-907F: все версии

EP-976A3: все версии  
EP-977A3: все версии  
EP-978A3: все версии  
EP-979A3: все версии  
EP-982A3: все версии  
EP-M552T: все версии  
EP-M570T: все версии  
EW-052A: все версии  
EW-452A: все версии  
EW-M5071FT: все версии  
EW-M530F: все версии  
EW-M5610FT: все версии  
EW-M571T: все версии  
EW-M571TW: все версии  
EW-M630TB: все версии  
EW-M630TW: все версии  
EW-M660FT: все версии  
EW-M670FT: все версии  
EW-M670FTW: все версии  
EW-M752T: все версии  
EW-M752TB: все версии  
EW-M770T: все версии  
EW-M770TW: все версии  
EW-M970A3T: все версии  
LX-10000: все версии  
LX-10000F: все версии  
LX-10010M: все версии  
LX-10010MF: все версии  
LX-10020M: все версии  
LX-10020MF: все версии  
LX-10050M: все версии  
LX-10050MF: все версии  
LX-6050M: все версии  
LX-6050MF: все версии

LX-7000: все версии  
LX-7000F: все версии  
LX-7550M: все версии  
LX-7550MF: все версии  
PF-70: все версии  
PF-71: все версии  
PF-81: все версии  
PM-T960: все версии  
PM-T990: все версии  
PX-046A: все версии  
PX-047A: все версии  
PX-048A: все версии  
PX-049A: все версии  
PX-105: все версии  
PX-1200: все версии  
PX-1600F: все версии  
PX-1700F: все версии  
PX-201: все версии  
PX-203: все версии  
PX-204: все версии  
PX-205: все версии  
PX-434A: все версии  
PX-435A: все версии  
PX-436A: все версии  
PX-437A: все версии  
PX-502A: все версии  
PX-503A: все версии  
PX-504A: все версии  
PX-505F: все версии  
PX-535F: все версии  
PX-5V: все версии  
PX-601F: все версии  
PX-602F: все версии  
PX-603F: все версии

PX-605F: все версии  
PX-673F: все версии  
PX-675F: все версии  
PX-7V: все версии  
PX-B310: все версии  
PX-B500: все версии  
PX-B510: все версии  
PX-B700: все версии  
PX-B750F: все версии  
PX-K150: все версии  
PX-K701: все версии  
PX-K751F: все версии  
PX-M160T: все версии  
PX-M270FT: все версии  
PX-M270T: все версии  
PX-M350F: все версии  
PX-M380F: все версии  
PX-M381FL: все версии  
PX-M5040F: все версии  
PX-M5041F: все версии  
PX-M5080F: все версии  
PX-M5081F: все версии  
PX-M6010F: все версии  
PX-M6011F: все версии  
PX-M650A: все версии  
PX-M650F: все версии  
PX-M6711FT: все версии  
PX-M6712FT: все версии  
PX-M680F: все версии  
PX-M7050F: все версии  
PX-M7050FP: все версии  
PX-M7050FT: все версии  
PX-M7050FX: все версии  
PX-M7070FX: все версии

PX-M7080FX: все версии  
PX-M7090FX: все версии  
PX-M7110F: все версии  
PX-M7110FP: все версии  
PX-M7110FT: все версии  
PX-M730F: все версии  
PX-M740F: все версии  
PX-M741F: все версии  
PX-M780F: все версии  
PX-M781F: все версии  
PX-M791FT: все версии  
PX-M840F: все версии  
PX-M840FX: все версии  
PX-M860F: все версии  
PX-M880FX: все версии  
PX-M884F: все версии  
PX-M885F: все версии  
PX-M886FL: все версии  
PX-S05B: все версии  
PX-S05BK: все версии  
PX-S05W: все версии  
PX-S06B: все версии  
PX-S06BK: все версии  
PX-S06W: все версии  
PX-S160T: все версии  
PX-S170T: все версии  
PX-S270T: все версии  
PX-S350: все версии  
PX-S380: все версии  
PX-S381L: все версии  
PX-S5010: все версии  
PX-S5040: все версии  
PX-S5080: все версии  
PX-S6010: все версии

PX-S6710T: все версии  
PX-S7050: все версии  
PX-S7050PS: все версии  
PX-S7050X: все версии  
PX-S7070X: все версии  
PX-S7090X: все версии  
PX-S7110: все версии  
PX-S7110P: все версии  
PX-S740: все версии  
PX-S840: все версии  
PX-S840X: все версии  
PX-S860: все версии  
PX-S880X: все версии  
PX-S884: все версии  
PX-S885: все версии  
SC-PX1V: все версии  
SC-PX1VL: все версии  
SC-PX3V: все версии  
SC-PX5V2: все версии  
SC-PX7V2: все версии  
LP-8200C: все версии  
LP-8500C: все версии  
LP-8700PS3: все версии  
LP-9200B: все версии  
LP-9200C: все версии  
LP-9200PS2: все версии  
LP-9200PS3: все версии  
LP-9300: все версии  
LP-9600: все версии  
LP-9600S: все версии  
LP-9800C: все версии  
LP-A500: все версии  
LP-A500F: все версии  
LP-M5000: все версии

LP-M5300: все версии  
LP-M6000: все версии  
LP-M8040: все версии  
LP-M8170: все версии  
LP-M8180: все версии  
LP-S180DN: все версии  
LP-S2290: все версии  
LP-S280DN: все версии  
LP-S3000: все версии  
LP-S3000PS: все версии  
LP-S300N: все версии  
LP-S310N: все версии  
LP-S3200: все версии  
LP-S3250: все версии  
LP-S3290: все версии  
LP-S340DN: все версии  
LP-S3500: все версии  
LP-S3550: все версии  
LP-S3590: все версии  
LP-S380DN: все версии  
LP-S4000: все версии  
LP-S4200: все версии  
LP-S4250: все версии  
LP-S4290: все версии  
LP-S440DN: все версии  
LP-S4500: все версии  
LP-S5000: все версии  
LP-S5300: все версии  
LP-S5500: все версии  
LP-S6000: все версии  
LP-S6160: все версии  
LP-S6500: все версии  
LP-S7000: все версии  
LP-S7100: все версии

LP-S7160: все версии  
LP-S7180: все версии  
LP-S7500: все версии  
LP-S8100: все версии  
LP-S8160: все версии  
LP-S8180: все версии  
LP-S9000: все версии  
LP-S9070: все версии  
LP-S950: все версии  
LP-V500: все версии  
VP-D1800N: все версии  
VP-D800N: все версии  
VP-F4400N: все версии  
GS6000: все версии  
PX-20000: все версии  
PX-5002: все версии  
PX-5800: все версии  
PX-6250S: все версии  
PX-6550: все версии  
PX-7500N: все версии  
PX-7550: все версии  
PX-7550S: все версии  
PX-9500N: все версии  
PX-9550: все версии  
PX-9550S: все версии  
PX-F10000: все версии  
PX-F8000: все версии  
PX-H10000: все версии  
PX-H6000: все версии  
PX-H7000: все версии  
PX-H8000: все версии  
PX-H9000: все версии  
PX-W8000: все версии  
SC-F10050: все версии

SC-F10050H: все версии  
SC-F150: все версии  
SC-F2000: все версии  
SC-F2150: все версии  
SC-F3050: все версии  
SC-F550: все версии  
SC-F551: все версии  
SC-F6000: все версии  
SC-F6200: все версии  
SC-F6350: все версии  
SC-F7100: все версии  
SC-F7200: все версии  
SC-F9200: все версии  
SC-F9350: все версии  
SC-F9450: все версии  
SC-F9450H: все версии  
SC-P10050: все версии  
SC-P20050: все версии  
SC-P5050: все версии  
SC-P6050: все версии  
SC-P7050: все версии  
SC-P7550: все версии  
SC-P8050: все версии  
SC-P9050: все версии  
SC-P9550: все версии  
SC-R5050: все версии  
SC-R5050L: все версии  
SC-S30650: все версии  
SC-S40650: все версии  
SC-S50650: все версии  
SC-S60650: все версии  
SC-S60650L: все версии  
SC-S70650: все версии  
SC-S80650: все версии

SC-S80650L: все версии  
SC-T2150: все версии  
SC-T3050: все версии  
SC-T3150: все версии  
SC-T3150M: все версии  
SC-T3150N: все версии  
SC-T3150X: все версии  
SC-T3250: все версии  
SC-T3255: все версии  
SC-T3450: все версии  
SC-T3450N: все версии  
SC-T3455: все версии  
SC-T3455N: все версии  
SC-T5050: все версии  
SC-T5150: все версии  
SC-T5150M: все версии  
SC-T5150N: все версии  
SC-T5250: все версии  
SC-T5250D: все версии  
SC-T5255: все версии  
SC-T5255D: все версии  
SC-T5450: все версии  
SC-T5450M: все версии  
SC-T5455: все версии  
SC-T7050: все версии  
SC-T7250: все версии  
SC-T7250D: все версии  
SC-T7255: все версии  
SC-T7255D: все версии  
TM-T70-i: все версии  
TM-T88 **V**-i: все версии  
DS-360W: все версии  
DS-40: все версии  
DS-560: все версии

DS-570W: все версии  
DS-571W: все версии  
DS-780N: все версии  
FF-680W: все версии  
DSBXNW1: все версии  
DSPNNW1: все версии  
ESIFNW1: все версии  
ESNSB1: все версии  
ESNSB2: все версии  
PA-W11G: все версии  
PA-W11G2: все версии  
PRIFNW1: все версии  
PRIFNW1S: все версии  
PRIFNW2: все версии  
PRIFNW2AC: все версии  
PRIFNW2S: все версии  
PRIFNW2SAC: все версии  
PRIFNW3: все версии  
PRIFNW3S: все версии  
PRIFNW6: все версии  
PRIFNW7: все версии  
PRIFNW7S: все версии  
PRIFNW7U: все версии

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Не определено

**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: 2024-09-30 / 2024-09-30

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU95133448/index.html>
- [http://www.epson.jp/support/misc\\_t/240930\\_03\\_oshirase.htm](http://www.epson.jp/support/misc_t/240930_03_oshirase.htm)

**Краткое описание:** Получение конфиденциальной информации в Cisco DNA Center

**Идентификатор уязвимости:** CVE-2024-20350  
BDU:2024-07524

**Идентификатор программной ошибки:** CWE-321 Использование жестко закодированного ключа шифрования

**Уязвимый продукт:** Cisco DNA Center: 2.3.3 - 2.3.7

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** Получение конфиденциальной информации

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ssh-e4uOdASj>
- <https://bdu.fstec.ru/vul/2024-07524>

**Краткое описание:** Отказ в обслуживании в Cisco IOS XE Software IPv4 fragmentation reassembly

**Идентификатор уязвимости:** CVE-2024-20467

**Идентификатор программной ошибки:** CWE-399 Уязвимости, связанные с управлением ресурсами

**Уязвимый продукт:** Cisco IOS XE: 17.12.1 - 17.12.1a

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Отказ в обслуживании

3

**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:** 2024-09-25 / 2024-09-25

**Ссылки на источник:**

- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpp-vfr-dos-nhHKGgO>
- <http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh44152>

**Краткое описание:** Получение конфиденциальной информации в AdaCore aws

**Идентификатор уязвимости:** CVE-2024-41708

**Идентификатор программной ошибки:** CWE-337 Предсказуемое начальное значение ГПСЧ

**Уязвимый продукт:** aws: 2.9.0 - 24.0.0

**Категория уязвимого продукта:** Универсальные компоненты и библиотеки

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** Получение конфиденциальной информации

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

**Оценка CVSSv3:** 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N/E:U/RL:U/RC:C

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-27 / 2024-09-27

**Ссылки на источник:**

- <http://docs.adacore.com/corp/security-advisories/SEC.AWS-0040-v2.pdf>

**Краткое описание:** Выполнение произвольного кода в PHP

**Идентификатор уязвимости:** CVE-2024-8926

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

**Уязвимый продукт:** PHP: 8.0.0 - 8.3.11

**Категория уязвимого продукта:** Универсальные компоненты и библиотеки

**Способ эксплуатации:** Отправка специально созданного HTTP-запроса.

**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:** 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:** 2024-09-27 / 2024-09-27

**Ссылки на источник:**

- <http://www.php.net/ChangeLog-8.php#8.1.30>
- <http://www.php.net/ChangeLog-8.php#8.2.24>
- <http://www.php.net/ChangeLog-8.php#8.3.12>

**Краткое описание:** Выполнение произвольного кода в HPE Aruba Networking Access Points

**Идентификатор уязвимости:** CVE-2024-42507

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

**Уязвимый продукт:** ArubaOS: до 10.7.0.0

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

**Способ эксплуатации:** Некорректная проверка входных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

**6 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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- [http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04712en\\_us&docLocale=en\\_US](http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04712en_us&docLocale=en_US)

**Краткое описание:** Выполнение произвольного кода в HPE Aruba Networking Access Points

**Идентификатор уязвимости:** CVE-2024-42506

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

**Уязвимый продукт:** ArubaOS: до 10.7.0.0

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

**Способ эксплуатации:** Некорректная проверка входных 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:** 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- [http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04712en\\_us&docLocale=en\\_US](http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04712en_us&docLocale=en_US)

**Краткое описание:** Выполнение произвольного кода в HPE Aruba Networking Access Points

**Идентификатор уязвимости:** CVE-2024-42505

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

**Уязвимый продукт:** ArubaOS: до 10.7.0.0

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

**Способ эксплуатации:** Некорректная проверка входных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

8 **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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- [http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04712en\\_us&docLocale=en\\_US](http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04712en_us&docLocale=en_US)

**Краткое описание:** Выполнение произвольного кода в Service Interconnect 1

**Идентификатор уязвимости:** CVE-2024-45492  
BDU:2024-07376

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

**Уязвимый продукт:** Service Interconnect: до 1.4

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://access.redhat.com/errata/RHSA-2024:7213>
- <https://bdu.fstec.ru/vul/2024-07376>

**Краткое описание:** Выполнение произвольного кода в Service Interconnect 1

**Идентификатор уязвимости:** CVE-2024-45491  
BDU:2024-07377

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

**Уязвимый продукт:** Service Interconnect: до 1.4

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

10 **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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://access.redhat.com/errata/RHSA-2024:7213>
- <https://bdu.fstec.ru/vul/2024-07377>

**Краткое описание:** Выполнение произвольного кода в Service Interconnect 1

**Идентификатор уязвимости:** CVE-2024-45490  
BDU:2024-07004

**Идентификатор программной ошибки:** CWE-124 Запись данных в область перед началом буфера

**Уязвимый продукт:** Service Interconnect: до 1.4

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Отправка специально сформированных данных.

**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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://access.redhat.com/errata/RHSA-2024:7213>
- <https://bdu.fstec.ru/vul/2024-07004>

**Краткое описание:** Отказ в обслуживании в Service Interconnect 1

**Идентификатор уязвимости:** CVE-2024-6119  
BDU:2024-06735

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

**Уязвимый продукт:** Service Interconnect: до 1.4

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Отказ в обслуживании

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:** Не определено

**Вектор атаки:** Не определено

**Взаимодействие с пользователем:** Не определено

**Дата выявления / Дата обновления:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://access.redhat.com/errata/RHSA-2024:7213>
- <https://bdu.fstec.ru/vul/2024-06735>

**Краткое описание:** Выполнение произвольного кода в Service Interconnect 1

**Идентификатор уязвимости:** CVE-2024-6345  
BDU:2024-05843

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

**Уязвимый продукт:** Service Interconnect: до 1.4

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Отправка специально созданных запросов.

**Последствия эксплуатации:** Выполнение произвольного кода

13 **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:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://access.redhat.com/errata/RHSA-2024:7213>
- <https://bdu.fstec.ru/vul/2024-05843>

Краткое описание: Обход безопасности в Service Interconnect 1

Идентификатор уязвимости: CVE-2024-37370  
BDU:2024-07016

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Service Interconnect: до 1.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 2024-09-26 / 2024-09-26

Ссылки на источник:

- <http://access.redhat.com/errata/RHSA-2024:7213>
- <https://bdu.fstec.ru/vul/2024-07016>

**Краткое описание:** Получение конфиденциальной информации в Service Interconnect 1

**Идентификатор уязвимости:** CVE-2024-37371  
BDU:2024-07005

**Идентификатор программной ошибки:** CWE-125 Чтение за пределами буфера

**Уязвимый продукт:** Service Interconnect: до 1.4

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Получение конфиденциальной информации

15 **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:H/I:N/A:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://access.redhat.com/errata/RHSA-2024:7213>
- <https://bdu.fstec.ru/vul/2024-07005>

Краткое описание: Отказ в обслуживании в Cisco Catalyst SD-WAN Routers

Идентификатор уязвимости: CVE-2024-20455

Идентификатор программной ошибки: CWE-371 Уязвимости, связанные с состоянием

Уязвимый продукт: Cisco IOS XE: 17.9.3a  
Cisco 1000 Series Integrated Services Routers: все версии  
Catalyst 8000V Edge Software: все версии  
Catalyst 8200 Series Edge Platforms: все версии  
Catalyst 8300 Series Edge Platforms: все версии  
Catalyst 8500L Series Edge Platforms: все версии  
Catalyst IR8300 Rugged Series Routers: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

16 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: 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: 2024-09-26 / 2024-09-26

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-utd-dos-hDATqxs>

**Краткое описание:** Отказ в обслуживании в Cisco IOS and IOS XE Software

**Идентификатор уязвимости:** CVE-2024-20433

**Идентификатор программной ошибки:** CWE-121 Переполнение буфера в стеке

**Уязвимый продукт:** Cisco IOS Software: до Dublin-17.12.4  
Cisco IOS XE: до Dublin-17.12.4

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Переполнение буфера.

**Последствия эксплуатации:** Отказ в обслуживании

17 **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:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rsvp-dos-OypvgVZf>

**Краткое описание:** Отказ в обслуживании в Cisco IOS XE Software

**Идентификатор уязвимости:** CVE-2024-20436

**Идентификатор программной ошибки:** CWE-476 Разыменование нулевого указателя

**Уязвимый продукт:** Cisco IOS XE: 16.6.9 - 17.6.6

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Отказ в обслуживании

18 **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:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-httpsrvr-dos-yOZThut>

**Краткое описание:** Отказ в обслуживании в Cisco IOS XE Software

**Идентификатор уязвимости:** CVE-2024-20464

**Идентификатор программной ошибки:** CWE-20 Некорректная проверка входных данных

**Уязвимый продукт:** Cisco IOS XE: 17.13.1 - 17.13.1a

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Отказ в обслуживании

- 19 **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:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pim-APbVfySJ>

**Краткое описание:** Отказ в обслуживании в Cisco IOS XE Software

**Идентификатор уязвимости:** CVE-2024-20480

**Идентификатор программной ошибки:** CWE-783 Уязвимость, связанная с приоритетом операторов

**Уязвимый продукт:** Cisco IOS XE: 17.12.2

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Отказ в обслуживании

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:** 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:** 2024-09-26 / 2024-09-26

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sda-edge-dos-MBcbG9k>

**Краткое описание:** Выполнение произвольного кода в ZNC

**Идентификатор уязвимости:** CVE-2024-39844

**Идентификатор программной ошибки:** CWE-20 Некорректная проверка входных данных

**Уязвимый продукт:** ZNC: 1.6.1 rc1 - 1.9.0

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-09-25 / 2024-09-25

**Ссылки на источник:**

- <http://wiki.znc.in/Category:ChangeLog>
- <http://github.com/znc/znc/releases/tag/znc-1.9.1>
- <http://wiki.znc.in/ChangeLog/1.9.1>
- <http://www.openwall.com/lists/oss-security/2024/07/03/9>
- <http://www.openwall.com/lists/oss-security/2024/07/03/9>

**Краткое описание:** Обход безопасности в OPW Fuel Management Systems SiteSentinel

**Идентификатор уязвимости:** CVE-2024-8310

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

**Уязвимый продукт:** SiteSentinel: до 17Q2.1

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Обход процесса аутентификации

**Последствия эксплуатации:** Обход безопасности

22 **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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-25 / 2024-09-25

**Ссылки на источник:**

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-268-01>

**Краткое описание:** Выполнение произвольного кода в Nessus Network Monitor

**Идентификатор уязвимости:** CVE-2024-6197  
BDU:2024-06023

**Идентификатор программной ошибки:** CWE-415 Двойное освобождение

**Уязвимый продукт:** Nessus Network Monitor: 6.0.0 - 6.4.1

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Использование специально созданного вредоносного сертификата.

**Последствия эксплуатации:** Выполнение произвольного кода

23 **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:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- <http://www.tenable.com/security/tns-2024-17>
- <https://bdu.fstec.ru/vul/2024-06023>

**Краткое описание:** Выполнение произвольного кода в Nessus Network Monitor

**Идентификатор уязвимости:** CVE-2024-45492  
BDU:2024-07376

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

**Уязвимый продукт:** Nessus Network Monitor: 6.0.0 - 6.4.1

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

24

**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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- <http://www.tenable.com/security/tns-2024-17>
- <https://bdu.fstec.ru/vul/2024-07376>

**Краткое описание:** Выполнение произвольного кода в Nessus Network Monitor

**Идентификатор уязвимости:** CVE-2024-45491  
BDU:2024-07377

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

**Уязвимый продукт:** Nessus Network Monitor: 6.0.0 - 6.4.1

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

25 **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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- <http://www.tenable.com/security/tns-2024-17>
- <https://bdu.fstec.ru/vul/2024-07377>

**Краткое описание:** Отказ в обслуживании в Nessus Network Monitor

**Идентификатор уязвимости:** CVE-2024-6119  
BDU:2024-06735

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

**Уязвимый продукт:** Nessus Network Monitor: 6.0.0 - 6.4.1

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Использование специально созданного вредоносного сертификата.

**Последствия эксплуатации:** Отказ в обслуживании

26

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- <http://www.tenable.com/security/tns-2024-17>
- <https://bdu.fstec.ru/vul/2024-06735>

**Краткое описание:** Выполнение произвольного кода в Google Chrome и Microsoft Edge

**Идентификатор уязвимости:** CVE-2024-9123

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

**Уязвимый продукт:** Google Chrome: 100.0.4896.60 - 129.0.6668.59  
Microsoft Edge: 79.0.309.71 - 129.0.2792.52

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Выполнение произвольного кода

27

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop\\_24.html](http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_24.html)
- <http://crbug.com/365884464>
- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-9123>

**Краткое описание:** Выполнение произвольного кода в Google Chrome и Microsoft Edge

**Идентификатор уязвимости:** CVE-2024-9122

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

**Уязвимый продукт:** Google Chrome: 100.0.4896.60 - 129.0.6668.59  
Microsoft Edge: 79.0.309.71 - 129.0.2792.52

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Выполнение произвольного кода

28

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop\\_24.html](http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_24.html)
- <http://crbug.com/365802567>
- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-9122>

**Краткое описание:** Выполнение произвольного кода в Google Chrome и Microsoft Edge

**Идентификатор уязвимости:** CVE-2024-9120

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Google Chrome: 100.0.4896.60 - 129.0.6668.59  
Microsoft Edge: 79.0.309.71 - 129.0.2792.52

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Выполнение произвольного кода

29

**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:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop\\_24.html](http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_24.html)
- <http://crbug.com/365254285>
- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-9120>

**Краткое описание:** Выполнение произвольного кода в DataEase

**Идентификатор уязвимости:** CVE-2024-46997

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

**Уязвимый продукт:** DataEase: 2.0.0 - 2.10.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

30 **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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- <http://github.com/dataease/dataease/security/advisories/GHSA-h7mj-m72h-qm8w>

**Краткое описание:** Получение конфиденциальной информации в DataEase

**Идентификатор уязвимости:** CVE-2024-46985

**Идентификатор программной ошибки:** CWE-611 Некорректное ограничение ссылок на внешние сущности XML

**Уязвимый продукт:** DataEase: 2.0.0 - 2.10.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально созданного вредоносного XML-кода.

**Последствия эксплуатации:** Получение конфиденциальной информации

31

**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:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- <http://github.com/dataease/dataease/security/advisories/GHSA-4m9p-7xg6-f4mm>

Краткое описание: Выполнение произвольного кода в FastStone Image Viewer

Идентификатор уязвимости: CVE-2024-9114

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Image Viewer: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-24 / 2024-09-24

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1275/>

33

**Краткое описание:** Выполнение произвольного кода в FastStone Image Viewer

**Идентификатор уязвимости:** CVE-2024-9113

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Image Viewer: все версии

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

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

**Оценка CVSSv3:** 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1274/>

34

**Краткое описание:** Выполнение произвольного кода в FastStone Image Viewer

**Идентификатор уязвимости:** CVE-2024-9112

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Image Viewer: все версии

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

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

**Оценка CVSSv3:** 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1273/>

**Краткое описание:** Выполнение произвольного кода в Google ChromeOS

**Идентификатор уязвимости:** CVE-2024-8198  
BDU:2024-06725

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

**Уязвимый продукт:** Chrome OS: до 126.0.6478.253

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

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

35

**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:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for\\_23.html](http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for_23.html)
- <https://bdu.fstec.ru/vul/2024-06725>

**Краткое описание:** Выполнение произвольного кода в Google ChromeOS

**Идентификатор уязвимости:** CVE-2024-8193  
BDU:2024-07374

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

**Уязвимый продукт:** Chrome OS: до 126.0.6478.253

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

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

36

**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:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for\\_23.html](http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for_23.html)
- <https://bdu.fstec.ru/vul/2024-07374>

**Краткое описание:** Выполнение произвольного кода в Google ChromeOS

**Идентификатор уязвимости:** CVE-2024-7967  
BDU:2024-06553

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

**Уязвимый продукт:** Chrome OS: до 126.0.6478.253

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

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

37 **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:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for\\_23.html](http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for_23.html)
- <https://bdu.fstec.ru/vul/2024-06553>

**Краткое описание:** Выполнение произвольного кода в Google ChromeOS

**Идентификатор уязвимости:** CVE-2024-8362  
BDU:2024-07375

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Chrome OS: до 126.0.6478.253

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

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

**Последствия эксплуатации:** Выполнение произвольного кода

38 **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:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for\\_23.html](http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for_23.html)
- <https://bdu.fstec.ru/vul/2024-07375>

**Краткое описание:** Выполнение произвольного кода в Google ChromeOS

**Идентификатор уязвимости:** CVE-2024-6989  
BDU:2024-05892

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Chrome OS: до 126.0.6478.253

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

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

**Последствия эксплуатации:** Выполнение произвольного кода

39 **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:** 2024-09-24 / 2024-09-24

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for\\_23.html](http://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for_23.html)
- <https://bdu.fstec.ru/vul/2024-05892>

**Краткое описание:** Выполнение произвольного кода в BlueZ

**Идентификатор уязвимости:** CVE-2024-8805

**Идентификатор программной ошибки:** CWE-284 Некорректное управление доступом

**Уязвимый продукт:** BlueZ: все версии

**Категория уязвимого продукта:** Универсальные компоненты и библиотеки

**Способ эксплуатации:** Обход ограничений безопасности

**Последствия эксплуатации:** Выполнение произвольного кода

40

**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:** 2024-09-23 / 2024-09-23

**Ссылки на источник:**

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1229/>
- <http://patchwork.kernel.org/project/bluetooth/patch/20240912204458.3037144-1-luiz.dentz@gmail.com/>

**Краткое описание:** Выполнение произвольного кода в Rockwell Automation RSLogix 5 and RSLogix 500

**Идентификатор уязвимости:** CVE-2024-7847  
BDU:2024-07285

**Идентификатор программной ошибки:** CWE-345 Некорректная проверка достоверности данных

**Уязвимый продукт:** RSLogix 500: все версии  
RSLogix Micro Developer and Starter: все версии  
RSLogix 5: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**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:** 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:U/RC:C

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-09-23 / 2024-09-23

**Ссылки на источник:**

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-263-01>
- <http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1701.html>
- <https://bdu.fstec.ru/vul/2024-07285>

**Краткое описание:** Выполнение произвольного кода в F5 Traffix SDC Linux kernel

**Идентификатор уязвимости:** CVE-2023-45871  
BDU:2023-06999

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

**Уязвимый продукт:** Traffix SDC: 5.2.0 - 5.2.5

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

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

**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

**Дата выявления / Дата обновления:** 2024-09-23 / 2024-09-23

**Ссылки на источник:**

- <http://my.f5.com/manage/s/article/K000140865>
- <https://bdu.fstec.ru/vul/2023-06999>