# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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



## Бюллетень об уязвимостях программного обеспечения

VULN.2023-10-18.1 | 18 октября 2023 года

TLP: WHITE

# Перечень уязвимостей

| № п/п | Опасность | Идентификатор | Уязвимый продукт | Вектор атаки | Последствия | Дата выявления | Наличие обновления |
|---|---|---|---|---|---|---|---|
| 1 | Критическая | CVE-2023-5391 | Schneider Electric EcoStruxure Power Monitoring Expert and Power Operation Products | Сетевой | ACE | 2023-10-18 | ✓ |
| 2 | Высокая | CVE-2023-29464 | Rockwell Automation FactoryTalk Linx | Сетевой | DoS | 2023-10-18 | ✓ |
| 3 | Критическая | CVE-2023-34034 | MySQL Enterprise Monitor | Сетевой | SB | 2023-10-17 | ✓ |
| 4 | Высокая | CVE-2023-22102 | MySQL Connectors | Сетевой | ACE | 2023-10-17 | ✓ |
| 5 | Высокая | CVE-2023-38039 | Oracle Database Server | Сетевой | DoS | 2023-10-17 | ✓ |
| 6 | Высокая | CVE-2023-39331 | Node.js | Локальный | RLF | 2023-10-17 | ✓ |
| 7 | Критическая | CVE-2023-39332 | Node.js | Сетевой | RLF | 2023-10-17 | ✓ |
| 8 | Высокая | CVE-2023-20254 | Cisco Catalyst SD-WAN Manager | Сетевой | DoS | 2023-09-29 | ✓ |
| 9 | Критическая | CVE-2023-20198 | Cisco IOS XE | Сетевой | ACE | 2023-10-17 | ✗ |
| 10 | Критическая | CVE-2023-24479 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 11 | Критическая | CVE-2023-34426 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 12 | Критическая | CVE-2023-32645 | Yifan YF325 | Сетевой | SB | 2023-10-16 | ✗ |
| 13 | Высокая | CVE-2023-32632 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | Критическая | CVE-2023-34346 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 15 | Высокая | CVE-2023-35055 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 16 | Высокая | CVE-2023-35056 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 17 | Высокая | CVE-2023-31272 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 18 | Критическая | CVE-2023-34365 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 19 | Критическая | CVE-2023-35968 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 20 | Критическая | CVE-2023-35967 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 21 | Критическая | CVE-2023-35966 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 22 | Критическая | CVE-2023-35965 | Yifan YF325 | Сетевой | ACE | 2023-10-16 | ✗ |
| 23 | Высокая | CVE-2023-45158 | web2py | Сетевой | ACE | 2023-10-16 | ✓ |
| 24 | Высокая | CVE-2023-5218 | Microsoft Edge | Сетевой | ACE | 2023-10-14 | ✓ |
| 25 | Высокая | CVE-2023-5474 | Microsoft Edge | Сетевой | ACE | 2023-10-14 | ✓ |
| 26 | Высокая | CVE-2023-5476 | Microsoft Edge | Сетевой | OSI | 2023-10-14 | ✓ |

**Краткое описание:** Выполнение произвольного кода в Schneider Electric EcoStruxure Power Monitoring Expert and Power Operation Products

**Идентификатор уязвимости:** CVE-2023-5391

**Идентификатор программной ошибки:** CWE-502 Десериализация недоверенных данных

**Уязвимый продукт:** Schneider Electric EcoStruxure Power Monitoring Expert and Power Operation Products:
EcoStruxure Power Monitoring Expert: до 2023 hotfix 145271
EcoStruxure Power Operation with Advanced Reports: до 2022 hotfix 145271
EcoStruxure Power SCADA Operation with Advanced Reports: до 2022 hotfix 145271

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

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

**Последствия эксплуатации:** выполнение произвольного кода

1

**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:** 2023-10-18 / 2023-10-18

**Ссылки на источник:**

- http://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-283-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-283-02.pdf
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-290-01
- https://bdu.fstec.ru/vul/2023-06565

2

**Краткое описание:** Отказ в обслуживании в Rockwell Automation FactoryTalk Linx

**Идентификатор уязвимости:** CVE-2023-29464

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

**Уязвимый продукт:** Rockwell Automation FactoryTalk Linx: 6.20

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-18 / 2023-10-18

**Ссылки на источник:**

- http://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1141040
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-290-02

3

**Краткое описание:** Обход безопасности в MySQL Enterprise Monitor

**Идентификатор уязвимости:** CVE-2023-34034

**Идентификатор программной ошибки:** CWE-254 Уязвимости в безопасности ПО

**Уязвимый продукт:** MySQL Enterprise Monitor: 8.0.0 - 8.0.35

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

**Способ эксплуатации:** Не определено

**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:** 9.1 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:** 2023-10-17 / 2023-10-17

**Ссылки на источник:**

- http://www.oracle.com/security-alerts/cpuoct2023.html?61473
- https://bdu.fstec.ru/vul/2023-03799

4

**Краткое описание:** Выполнение произвольного кода в MySQL Connectors

**Идентификатор уязвимости:** CVE-2023-22102

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

**Уязвимый продукт:** MySQL Connectors: 8.0.7 - 8.1.0

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**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:** 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2023-10-17 / 2023-10-17

**Ссылки на источник:**

- http://www.oracle.com/security-alerts/cpuoct2023.html?3382

5

**Краткое описание:** Отказ в обслуживании в Oracle Database Server

**Идентификатор уязвимости:** CVE-2023-38039

**Идентификатор программной ошибки:** CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

**Уязвимый продукт:** Oracle Database Server: 21.3 - none

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

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

**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:** 2023-10-17 / 2023-10-17

**Ссылки на источник:**

- http://www.oracle.com/security-alerts/cpuoct2023.html?1408
- https://bdu.fstec.ru/vul/2023-05819

6

**Краткое описание:** Чтение локальных файлов в Node.js

**Идентификатор уязвимости:** CVE-2023-39331

**Идентификатор программной ошибки:** CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

**Уязвимый продукт:** Node.js: 20.0.0 - 20.8.0

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

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

**Последствия эксплуатации:** чтение локальных файлов

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-17 / 2023-10-17

**Ссылки на источник:**

- http://nodejs.org/en/blog/vulnerability/october-2023-security-releases

**Краткое описание:** Чтение локальных файлов в Node.js

**Идентификатор уязвимости:** CVE-2023-39332

**Идентификатор программной ошибки:** CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

**Уязвимый продукт:** Node.js: 20.0.0 - 20.8.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** чтение локальных файлов

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:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-17 / 2023-10-17

**Ссылки на источник:**

- http://nodejs.org/en/blog/vulnerability/october-2023-security-releases

8

**Краткое описание:** Отказ в обслуживании в Cisco Catalyst SD-WAN Manager

**Идентификатор уязвимости:** CVE-2023-20254

**Идентификатор программной ошибки:** CWE-285 Некорректная авторизация

**Уязвимый продукт:** Cisco Catalyst SD-WAN Manager: 20.3 - 20.11

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-09-29 / 2023-09-29

**Ссылки на источник:**

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vman-sc-LRLfu2z
- https://bdu.fstec.ru/vul/2023-06230

9

**Краткое описание:** Выполнение произвольного кода в Cisco IOS XE

**Идентификатор уязвимости:** CVE-2023-20198

**Идентификатор программной ошибки:** CWE-269 Некорректное управление привилегиями

**Уязвимый продукт:** Cisco IOS XE: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Последствия эксплуатации:** выполнение произвольного кода

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

**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:** 2023-10-17 / 2023-10-17

**Ссылки на источник:**

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh87343
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-24479

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Не определено

**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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1762

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-34426

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** выполнение произвольного кода

11 **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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1766

**Краткое описание:** Обход безопасности в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-32645

**Идентификатор программной ошибки:** CWE-489 Присутствует код отладки

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Последствия эксплуатации:** обход безопасности

12 **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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1752

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-32632

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** выполнение произвольного кода

13 **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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1767

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-34346

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** выполнение произвольного кода

14 **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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1764

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-35055

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** выполнение произвольного кода

15

**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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1761

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-35056

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** выполнение произвольного кода

16

**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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1761

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-31272

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** выполнение произвольного кода

17 **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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1765

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-34365

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** выполнение произвольного кода

18 **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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1763

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-35968

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Последствия эксплуатации:** выполнение произвольного кода

19

**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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1788

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-35967

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Последствия эксплуатации:** выполнение произвольного кода

20

**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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1788

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-35966

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Последствия эксплуатации:** выполнение произвольного кода

21

**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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1787

**Краткое описание:** Выполнение произвольного кода в Yifan YF325

**Идентификатор уязвимости:** CVE-2023-35965

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

**Уязвимый продукт:** Yifan YF325: 1.0_20221108

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Последствия эксплуатации:** выполнение произвольного кода

22 **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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1787

**Краткое описание:** Выполнение произвольного кода в web2py

**Идентификатор уязвимости:** CVE-2023-45158

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

**Уязвимый продукт:** web2py: 2.0.0 - 2.24.1

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**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:** 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:** 2023-10-16 / 2023-10-16

**Ссылки на источник:**

- http://jvn.jp/en/jp/JVN80476432/index.html

24

**Краткое описание:** Выполнение произвольного кода в Microsoft Edge

**Идентификатор уязвимости:** CVE-2023-5218

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

**Уязвимый продукт:** Microsoft Edge: 79.0.309.71 - 117.0.2045.60

**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:** 2023-10-14 / 2023-10-14

**Ссылки на источник:**

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-5218
- https://bdu.fstec.ru/vul/2023-06604

**Краткое описание:** Выполнение произвольного кода в Microsoft Edge

**Идентификатор уязвимости:** CVE-2023-5474

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

**Уязвимый продукт:** Microsoft Edge: 79.0.309.71 - 117.0.2045.60

**Категория уязвимого продукта:** Операционные системы Microsoft и их компоненты

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

**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:** 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:** 2023-10-14 / 2023-10-14

**Ссылки на источник:**

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-5474

**Краткое описание:** Получение конфиденциальной информации в Microsoft Edge

**Идентификатор уязвимости:** CVE-2023-5476

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

**Уязвимый продукт:** Microsoft Edge: 79.0.309.71 - 117.0.2045.60

**Категория уязвимого продукта:** Операционные системы Microsoft и их компоненты

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

**Последствия эксплуатации:** получение конфиденциальной информации

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:** 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:** 2023-10-14 / 2023-10-14

**Ссылки на источник:**

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-5476