НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-10-09.1 | 9 октября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-44419	D-Link DIR-X3260	Смежная сеть	ACE	2023-10-05	✗
2	Высокая	CVE-2023-44420	D-Link DIR-X3260	Смежная сеть	SB	2023-10-05	✗
3	Высокая	CVE-2023-44421	D-Link DIR-X3260	Смежная сеть	ACE	2023-10-05	✗
4	Высокая	CVE-2023-44422	D-Link DIR-X3260	Смежная сеть	ACE	2023-10-05	✗
5	Высокая	CVE-2023-44423	D-Link DIR-X3260	Смежная сеть	ACE	2023-10-05	✗
6	Высокая	CVE-2023-44424	D-Link DIR-X3260	Смежная сеть	ACE	2023-10-05	✗
7	Высокая	CVE-2023-44425	D-Link DIR-X3260	Смежная сеть	ACE	2023-10-05	✗
8	Высокая	CVE-2023-44426	D-Link DIR-X3260	Смежная сеть	ACE	2023-10-05	✗
9	Высокая	CVE-2023-44427	D-Link DIR-X3260	Смежная сеть	ACE	2023-10-05	✗
10	Высокая	CVE-2023-44418	D-Link DIR-X3260	Смежная сеть	ACE	2023-10-05	✗
11	Высокая	CVE-2023-42127	Kofax Power PDF Advanced	Локальный	ACE	2023-10-09	✓

12	Критическая	None	Microsoft PC Manager	Сетевой	ACE	2023-10-06	✓
13	Критическая	None	Microsoft PC Manager	Сетевой	ACE	2023-10-06	✓

1

Краткое описание: Выполнение произвольного кода в D-Link DIR-X3260

Идентификатор уязвимости: CVE-2023-44419

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DIR-X3260: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1517/
- https://bdu.fstec.ru/vul/2023-06367

2

Краткое описание: Обход безопасности в D-Link DIR-X3260

Идентификатор уязвимости: CVE-2023-44420

Идентификатор программной ошибки: CWE-303 Некорректная реализация алгоритма аутентификации

Уязвимый продукт: D-Link DIR-X3260: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: обход безопасности

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

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1518/
- https://bdu.fstec.ru/vul/2023-06368

3

Краткое описание: Выполнение произвольного кода в D-Link DIR-X3260

Идентификатор уязвимости: CVE-2023-44421

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: D-Link DIR-X3260: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1519/

4

Краткое описание: Выполнение произвольного кода в D-Link DIR-X3260

Идентификатор уязвимости: CVE-2023-44422

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: D-Link DIR-X3260: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1520/

Краткое описание: Выполнение произвольного кода в D-Link DIR-X3260

Идентификатор уязвимости: CVE-2023-44423

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: D-Link DIR-X3260: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

5

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1521/
- https://bdu.fstec.ru/vul/2023-06404

Краткое описание: Выполнение произвольного кода в D-Link DIR-X3260

Идентификатор уязвимости: CVE-2023-44424

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: D-Link DIR-X3260: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

6

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1522/
- https://bdu.fstec.ru/vul/2023-06405

7

Краткое описание: Выполнение произвольного кода в D-Link DIR-X3260

Идентификатор уязвимости: CVE-2023-44425

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: D-Link DIR-X3260: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1523/

8

Краткое описание: Выполнение произвольного кода в D-Link DIR-X3260

Идентификатор уязвимости: CVE-2023-44426

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: D-Link DIR-X3260: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1524/

9

Краткое описание: Выполнение произвольного кода в D-Link DIR-X3260

Идентификатор уязвимости: CVE-2023-44427

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: D-Link DIR-X3260: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1525/

Краткое описание: Выполнение произвольного кода в D-Link DIR-X3260

Идентификатор уязвимости: CVE-2023-44418

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

Уязвимый продукт: D-Link DIR-X3260: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1516/

11

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2023-42127

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Kofax Power PDF Advanced: до 5.0.0.14

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-10-09 / 2023-10-09

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1536/
- http://docshield.kofax.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.14.htm

Краткое описание: Выполнение произвольного кода в Microsoft PC Manager

Идентификатор уязвимости: None

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: Microsoft PC Manager: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

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: 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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1527/

Краткое описание: Выполнение произвольного кода в Microsoft PC Manager

Идентификатор уязвимости: None

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: Microsoft PC Manager: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

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: 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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1528/