НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-12-22.1 | 22 декабря 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-50234	Hancom Office	Локальный	ACE	2023-12-22	✗
2	Высокая	CVE-2023-50235	Hancom Office	Локальный	ACE	2023-12-22	✗
3	Высокая	CVE-2023-51598	Hancom Office	Локальный	ACE	2023-12-22	✗
4	Высокая	CVE-2023-51608	Kofax Power PDF	Локальный	ACE	2023-12-22	✗
5	Высокая	CVE-2023-51606	Kofax Power PDF	Локальный	ACE	2023-12-22	✗
6	Высокая	CVE-2023-51597	Kofax Power PDF	Локальный	ACE	2023-12-22	✗
7	Высокая	CVE-2023-50216	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
8	Высокая	CVE-2023-50215	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
9	Высокая	CVE-2023-50214	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
10	Высокая	CVE-2023-50213	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
11	Высокая	CVE-2023-50211	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
12	Высокая	CVE-2023-50210	D-Link G416	Смежная сеть	ACE	2023-12-21	✓

13	Высокая	CVE-2023-50209	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
14	Высокая	CVE-2023-50208	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
15	Высокая	CVE-2023-50207	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
16	Высокая	CVE-2023-50206	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
17	Высокая	CVE-2023-50205	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
18	Высокая	CVE-2023-50204	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
19	Высокая	CVE-2023-50203	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
20	Высокая	CVE-2023-50202	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
21	Высокая	CVE-2023-50198	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
22	Высокая	CVE-2023-50201	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
23	Высокая	CVE-2023-50200	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
24	Высокая	CVE-2023-50199	D-Link G416	Смежная сеть	SB	2023-12-21	✓

25	Высокая	CVE-2023-50217	D-Link G416	Смежная сеть	ACE	2023-12-21	✓
26	Высокая	CVE-2023-7024	Google Chrome	Сетевой	ACE	2023-12-21	✓
27	Критическая	CVE-2023-6930	EuroTel ETL3100 Radio Transmitter	Сетевой	OSI	2023-12-20	✗
28	Высокая	CVE-2023-6929	EuroTel ETL3100 Radio Transmitter	Сетевой	SB	2023-12-20	✗
29	Критическая	CVE-2023-6928	EuroTel ETL3100 Radio Transmitter	Сетевой	OSI	2023-12-20	✗
30	Высокая	CVE-2023-6873	Mozilla Firefox	Сетевой	ACE	2023-12-19	✓
31	Высокая	CVE-2023-6864	Mozilla Firefox и Mozilla Thunderbird	Сетевой	ACE	2023-12-19	✓
32	Высокая	CVE-2023-6856	Mozilla Firefox и Mozilla Thunderbird	Сетевой	ACE	2023-12-19	✓
33	Высокая	CVE-2023-50227	Parallels Desktop	Сетевой	ACE	2023-12-19	✓
34	Высокая	CVE-2023-50228	Parallels Desktop	Локальный	ACE	2023-12-19	✓
35	Высокая	CVE-2023-44487	HashiCorp Consul	Сетевой	DoS	2023-12-18	✓
36	Высокая	CVE-2023-45285	HashiCorp Consul	Сетевой	OSI	2023-12-18	✓
37	Высокая	CVE-2023-45283	HashiCorp Consul	Сетевой	SB	2023-12-18	✓
38	Высокая	CVE-2023-47539	FortiMail	Сетевой	SB	2023-12-15	✓

1

Краткое описание: Выполнение произвольного кода в Hancom Office

Идентификатор уязвимости: CVE-2023-50234

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Hancom Office: 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 межсетевого экранирования или другими административными мерами.

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: 2023-12-22 / 2023-12-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1856/

2

Краткое описание: Выполнение произвольного кода в Hancom Office

Идентификатор уязвимости: CVE-2023-50235

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Hancom Office: 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 межсетевого экранирования или другими административными мерами.

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: 2023-12-22 / 2023-12-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1857/

3

Краткое описание: Выполнение произвольного кода в Hancom Office

Идентификатор уязвимости: CVE-2023-51598

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Hancom Office: 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 межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.0 AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-12-22 / 2023-12-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1855/

4

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2023-51608

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

Уязвимый продукт: Power PDF Advanced: все версии
Power PDF Standard: 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 межсетевого экранирования или другими административными мерами.

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: 2023-12-22 / 2023-12-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1909/

5

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2023-51606

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Power PDF Advanced: все версии
Power PDF Standard: 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 межсетевого экранирования или другими административными мерами.

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: 2023-12-22 / 2023-12-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1907/

6

Краткое описание: Выполнение произвольного кода в Kofax Power PDF

Идентификатор уязвимости: CVE-2023-51597

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Power PDF Advanced: все версии
Power PDF Standard: 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 межсетевого экранирования или другими административными мерами.

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: 2023-12-22 / 2023-12-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1906/

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50216

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных 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: 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1832/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

8

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50215

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1831/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50214

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1830/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50213

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1829/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

11

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50211

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: G416: 1.08b02

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: 8.8 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1827/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

12

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50210

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: G416: 1.08b02

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: 8.8 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1826/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

13

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50209

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: G416: 1.08b02

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: 8.8 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1825/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

14

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50208

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: G416: 1.08b02

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: 8.8 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1824/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50207

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1823/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50206

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

16 **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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1822/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

17

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50205

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1821/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50204

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 8.8 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1820/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50203

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 8.8 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1819/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50202

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 8.8 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1818/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50198

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

21

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

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1814/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50201

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1817/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50200

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 8.8 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1816/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Обход безопасности в D-Link G416

Идентификатор уязвимости: CVE-2023-50199

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: обход безопасности

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: 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1815/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

Краткое описание: Выполнение произвольного кода в D-Link G416

Идентификатор уязвимости: CVE-2023-50217

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

Уязвимый продукт: G416: 1.08b02

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1833/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367

26

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-7024

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 120.0.6099.110

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-12-21 / 2023-12-21

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html
- http://crbug.com/1513170

Краткое описание: Получение конфиденциальной информации в EuroTel ETL3100 Radio Transmitter

Идентификатор уязвимости: CVE-2023-6930

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: ETL3100: 01c01 - 01x37

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: получение конфиденциальной информации

27

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

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-20 / 2023-12-20

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-353-05

Краткое описание: Обход безопасности в EuroTel ETL3100 Radio Transmitter

Идентификатор уязвимости: CVE-2023-6929

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: ETL3100: 01c01 - 01x37

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: обход безопасности

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

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: 2023-12-20 / 2023-12-20

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-353-05

Краткое описание: Получение конфиденциальной информации в EuroTel ETL3100 Radio Transmitter

Идентификатор уязвимости: CVE-2023-6928

Идентификатор программной ошибки: CWE-307 Некорректное ограничение количества неудачных попыток аутентификации

Уязвимый продукт: ETL3100: 01c01 - 01x37

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

29

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: 2023-12-20 / 2023-12-20

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-353-05

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2023-6873

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

Уязвимый продукт: Mozilla Firefox: 116.0 - 120.0.1
Firefox for Android: 116.0 - 120.1.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2023-12-19 / 2023-12-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2023-56/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Mozilla Thunderbird

Идентификатор уязвимости: CVE-2023-6864

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 120.0.1
Firefox ESR: 102.0 - 115.5.0
Firefox for Android: 66.0.4 - 120.1.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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: 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: 2023-12-19 / 2023-12-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2023-54/
- http://www.mozilla.org/en-US/security/advisories/mfsa2023-55/
- http://www.mozilla.org/en-US/security/advisories/mfsa2023-56/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Mozilla Thunderbird

Идентификатор уязвимости: CVE-2023-6856

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 120.0.1
Firefox ESR: 102.0 - 115.5.0
Firefox for Android: 66.0.4 - 120.1.1

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: выполнение произвольного кода

32 **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: 2023-12-19 / 2023-12-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2023-56/
- http://www.mozilla.org/en-US/security/advisories/mfsa2023-55/
- http://www.mozilla.org/en-US/security/advisories/mfsa2023-54/

33

Краткое описание: Выполнение произвольного кода в Parallels Desktop

Идентификатор уязвимости: CVE-2023-50227

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Parallels Desktop: до 19.1.0

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-12-19 / 2023-12-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1804/
- http://kb.parallels.com/en/125013

34

Краткое описание: Выполнение произвольного кода в Parallels Desktop

Идентификатор уязвимости: CVE-2023-50228

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Parallels Desktop: до 19.1.0

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

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-19 / 2023-12-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1803/
- http://kb.parallels.com/en/125013

35

Краткое описание: Отказ в обслуживании в HashiCorp Consul

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: Consul Enterprise: 1.17.0

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: 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: 2023-12-18 / 2023-12-18

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.17.1
- https://bdu.fstec.ru/vul/2023-06559

36

Краткое описание: Получение конфиденциальной информации в HashiCorp Consul

Идентификатор уязвимости: CVE-2023-45285

Идентификатор программной ошибки: CWE-311 Отсутствует шифрование важных данных

Уязвимый продукт: Consul Enterprise: 1.15.0 - 1.17.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 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: 2023-12-18 / 2023-12-18

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.16.4
- http://github.com/hashicorp/consul/releases/tag/v1.17.1

37

Краткое описание: Обход безопасности в HashiCorp Consul

Идентификатор уязвимости: CVE-2023-45283

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Consul Enterprise: 1.15.0 - 1.17.0

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: 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: 2023-12-18 / 2023-12-18

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.16.4
- http://github.com/hashicorp/consul/releases/tag/v1.17.1

38

Краткое описание: Обход безопасности в FortiMail

Идентификатор уязвимости: CVE-2023-47539

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Fortinet FortiMail: 7.4.0

Категория уязвимого продукта: Средства защиты информации

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: 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: 2023-12-15 / 2023-12-15

Ссылки на источник:

- http://www.fortiguard.com/psirt/FG-IR-23-439