НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-09-04.1 | 4 сентября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-39982	Moxa MXsecurity	Сетевой	OSI	2023-09-04	✓
2	Высокая	CVE-2023-39981	Moxa MXsecurity	Сетевой	SB	2023-09-04	✓
3	Критическая	CVE-2023-39979	Moxa MXsecurity	Сетевой	SB	2023-09-04	✓
4	Высокая	CVE-2023-4572	Microsoft Edge	Сетевой	ACE	2023-08-31	✓
5	Высокая	CVE-2023-41185	Unified Automation UaGateway	Сетевой	DoS	2023-08-31	✓
6	Высокая	CVE-2023-37324	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
7	Высокая	CVE-2023-37323	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
8	Высокая	CVE-2023-37322	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
9	Высокая	CVE-2023-37321	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
10	Высокая	CVE-2023-37320	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
11	Высокая	CVE-2023-37319	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓

12	Высокая	CVE-2023-37318	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
13	Высокая	CVE-2023-37317	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
14	Высокая	CVE-2023-37316	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
15	Высокая	CVE-2023-37315	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
16	Высокая	CVE-2023-37314	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
17	Высокая	CVE-2023-37312	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
18	Высокая	CVE-2023-37313	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
19	Высокая	CVE-2023-37311	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
20	Высокая	CVE-2023-37310	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
21	Высокая	CVE-2023-35758	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
22	Высокая	CVE-2023-35756	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
23	Высокая	CVE-2023-35755	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓

24	Высокая	CVE-2023-35754	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
25	Высокая	CVE-2023-35753	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
26	Высокая	CVE-2023-35752	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
27	Высокая	CVE-2023-35751	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
28	Высокая	CVE-2023-35748	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
29	Высокая	CVE-2023-35747	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
30	Высокая	CVE-2023-35746	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
31	Высокая	CVE-2023-35745	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
32	Высокая	CVE-2023-35744	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
33	Высокая	CVE-2023-35743	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
34	Высокая	CVE-2023-35742	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
35	Высокая	CVE-2023-35741	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓

36	Высокая	CVE-2023-35740	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
37	Высокая	CVE-2023-35739	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
38	Высокая	CVE-2023-35738	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
39	Высокая	CVE-2023-35737	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
40	Высокая	CVE-2023-35736	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
41	Высокая	CVE-2023-35735	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
42	Высокая	CVE-2023-35733	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
43	Высокая	CVE-2023-35732	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
44	Высокая	CVE-2023-35731	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
45	Высокая	CVE-2023-35730	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
46	Высокая	CVE-2023-35729	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
47	Высокая	CVE-2023-35728	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓

48	Высокая	CVE-2023-35727	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
49	Высокая	CVE-2023-35726	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
50	Высокая	CVE-2023-35724	D-Link DAP-2622	Смежная сеть	OSI	2023-08-30	✓
51	Высокая	CVE-2023-35725	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓
52	Высокая	CVE-2023-37326	D-Link DAP-2622	Смежная сеть	ACE	2023-08-30	✓

1

Краткое описание: Получение конфиденциальной информации в Moxa MXsecurity

Идентификатор уязвимости: CVE-2023-39982

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: Moxa MXsecurity: 1.0 - 1.0.1

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: 2023-09-04 / 2023-09-04

Ссылки на источник:

- http://www.moxa.com/en/support/product-support/security-advisory/mpsa-230403-mxsecurity-series-multiple-vulnerabilities
- https://bdu.fstec.ru/vul/2023-05089

2

Краткое описание: Обход безопасности в Moxa MXsecurity

Идентификатор уязвимости: CVE-2023-39981

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Moxa MXsecurity: 1.0 - 1.0.1

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: 2023-09-04 / 2023-09-04

Ссылки на источник:

- http://www.moxa.com/en/support/product-support/security-advisory/mpsa-230403-mxsecurity-series-multiple-vulnerabilities
- https://bdu.fstec.ru/vul/2023-05090

3

Краткое описание: Обход безопасности в Moxa MXsecurity

Идентификатор уязвимости: CVE-2023-39979

Идентификатор программной ошибки: CWE-334 Недостаточно большой диапазон случайных значений

Уязвимый продукт: Moxa MXsecurity: 1.0 - 1.0.1

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: 9.8 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: 2023-09-04 / 2023-09-04

Ссылки на источник:

- http://www.moxa.com/en/support/product-support/security-advisory/mpsa-230403-mxsecurity-series-multiple-vulnerabilities
- https://bdu.fstec.ru/vul/2023-05063

4

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-4572

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 116.0.1938.62

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: 2023-08-31 / 2023-08-31

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-4572

5

Краткое описание: Отказ в обслуживании в Unified Automation UaGateway

Идентификатор уязвимости: CVE-2023-41185

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

Уязвимый продукт: Unified Automation UaGateway: до 1.5.13

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: 8.6 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: 2023-08-31 / 2023-08-31

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1286/

6

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37324

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1278/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

7

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37323

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1277/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

8

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37322

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1276/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

9

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37321

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1275/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

10

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37320

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1274/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

11

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37319

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1273/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37318

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1272/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

13

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37317

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1271/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

14

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37316

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1270/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

15

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37315

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1269/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

16

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37314

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1268/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

17

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37312

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1266/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

18

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37313

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1267/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

19

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37311

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1265/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

20

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37310

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1264/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

21

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35758

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1263/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35756

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1261/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

23

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35755

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1260/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

24

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35754

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1259/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

25

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35753

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1258/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

26

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35752

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1257/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

27

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35751

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1256/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

28

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35748

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1254/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

29

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35747

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1252/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

30

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35746

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1251/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

31

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35745

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1250/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

32

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35744

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1249/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

33

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35743

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1248/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

34

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35742

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1247/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

35

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35741

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1246/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

36

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35740

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1245/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

37

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35739

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1244/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

38

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35738

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1243/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

39

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35737

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1242/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

40

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35736

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1241/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

41

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35735

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1240/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

42

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35733

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1239/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

43

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35732

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1238/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

44

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35731

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1237/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

45

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35730

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1236/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

46

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35729

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1235/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

47

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35728

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1234/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

48

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35727

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1233/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35726

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

49 **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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1232/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

Краткое описание: Получение конфиденциальной информации в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35724

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: D-Link DAP-2622: 1.00

Категория уязвимого продукта: Телекоммуникационное оборудование

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.

50

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1230/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349
- https://bdu.fstec.ru/vul/2023-04986

51

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-35725

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1231/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349

Краткое описание: Выполнение произвольного кода в D-Link DAP-2622

Идентификатор уязвимости: CVE-2023-37326

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-2622: 1.00

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

52 **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: 2023-08-30 / 2023-08-30

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1279/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349