

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2023-06-05.1 | 5 июня 2023 года

TLP: WHITE



Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Не определено	N/A	Gigabyte UEFI firmware	Не определено	ACE	2023-06-01	✗
2	Высокая	CVE-2023-32136	D-Link DAP-1360, DAP-2020	Смежная сеть	ACE	2023-05-04	✓
3	Высокая	CVE-2023-30063	D-Link DIR-890L	Сетевой	SB	2023-05-01	✗
4	Высокая	CVE-2023-30061	D-Link DIR-879	Сетевой	SB	2023-05-01	✗
5	Высокая	CVE-2023-2649	Tenda AC23	Сетевой	ACE	2023-05-11	✗
6	Критическая	CVE-2023-30135	Tenda AC18	Сетевой	DoS	2023-05-04	✗
7	Критическая	CVE-2023-29856	D-Link DIR-868L A1	Сетевой	SB	2023-05-02	✗

Краткое описание: Выполнение произвольного кода в Gigabyte UEFI firmware

Идентификатор уязвимости: N/A

Идентификатор программной ошибки: CWE-506 Внедренный вредоносный код

Уязвимый продукт: Gigabyte UEFI firmware:

A520M S2H rev 1.x: все версии
A620M GAMING X AX rev 1.0: все версии
A620M GAMING X rev 1.0: все версии
B360M DS3H rev 1.0: все версии
B365 HD3 rev 1.0: все версии
B365M DS3H rev 1.0: все версии
B450 AORUS Elite V2 rev 1.x: все версии
B450 AORUS M rev 1.x: все версии
B450 Gaming X rev 1.x: все версии
B450M AORUS ELITE rev 1.x: все версии
B450M DS3H rev 1.x: все версии
B450M DS3H V2 rev 1.x: все версии
B450M DS3H WIFI rev 1.x: все версии
B450M GAMING rev 1.x: все версии
B450M H rev 1.x: все версии
B450M K rev 1.0: все версии
B450M S2H rev 1.x: все версии
B460 AORUS PRO AC rev 1.0: все версии
B460 HD3 rev 1.0: все версии
B460M AORUS PRO rev 1.0: все версии
B460M D2V rev 1.0: все версии
B460M D3H rev 1.0: все версии
B460M DS3H AC rev 1.x: все версии
B460M DS3H rev 1.0: все версии
B460M GAMING HD rev 1.0: все версии
B460M POWER rev 1.0: все версии
B550 AORUS ELITE AX rev 1.0: все версии
B550 AORUS ELITE AX V2 rev 1.2: все версии
B550 AORUS ELITE AX V2 rev 1.2/1.3: все версии

B550 AORUS ELITE rev 1.0: все версии
B550 AORUS ELITE V2 rev 1.2: все версии
B550 GAMING X V2 rev 1.0/1.1/1.2: все версии
B550 GAMING X V2 rev 1.3: все версии
B550 GAMING X V2 rev 1.4: все версии
B550 Gaming X V2 rev 1.x: все версии
B550 UD AC rev 1.0 11: все версии
B550 UD AC rev 1.2: все версии
B550I AORUS PRO AX rev 1.0: все версии
B550I AORUS PRO AX rev 1.1: все версии
B550I AORUS PRO AX rev 1.2: все версии
B550M AORUS ELITE AX rev 1.3: все версии
B550M AORUS ELITE rev 1.0/1.1/1.2: все версии
B550M AORUS ELITE rev 1.3: все версии
B550M AORUS ELITE rev 1.x: все версии
B550M AORUS PRO AX rev 1.0: все версии
B550M AORUS PRO AX rev 1.1: все версии
B550M AORUS PRO P rev 1.0: все версии
B550M AORUS PRO P rev 1.1: все версии
B550M AORUS PRO P rev 1.2: все версии
B550M AORUS PRO rev 1.0: все версии
B550M DS3H AC rev 1.0/1.1/1.2/1.3: все версии
B550M DS3H AC rev 1.0/1.1/1.2/1.3/1.4: все версии
B550M DS3H AC rev 1.4: все версии
B550M DS3H AC rev 1.5 1.6: все версии
B550M DS3H AC rev 1.x: все версии
B550M DS3H rev 1.0/1.1/1.2/1.3: все версии
B550M DS3H rev 1.4: все версии
B550M DS3H rev 1.5: все версии
B550M DS3H rev 1.x: все версии
B550M GAMING rev 1.x: все версии
B550M K rev 1.0: все версии
B550M S2H rev 1.x: все версии
B560 AORUS PRO AX rev 1.0: все версии

B560 HD3 rev 1.x: все версии
B560I AORUS PRO AX rev 1.0: все версии
B560M AORUS ELITE rev 1.x: все версии
B560M AORUS PRO AX rev 1.x: все версии
B560M AORUS PRO rev 1.x: все версии
B560M D2V rev 1.x: все версии
B560M D3H rev 1.x: все версии
B560M DS3H AC rev 1.x: все версии
B560M DS3H PLUS rev 1.0: все версии
B560M DS3H V2 rev 1.0: все версии
B560M GAMING HD rev 1.x: все версии
B560M H rev 1.x: все версии
B560M H V2 rev 1.0: все версии
B560M POWER rev 1.x: все версии
B650 AERO G rev 1.0: все версии
B650 AORUS ELITE AX rev 1.x: все версии
B650 AORUS ELITE rev 1.0: все версии
B650 AORUS PRO AX rev 1.x: все версии
B650 GAMING X AX rev 1.0/1.1: все версии
B650 GAMING X AX rev 1.x: все версии
B650 GAMING X rev 1.0: все версии
B650 GAMING X rev 1.0 11: все версии
B650E AORUS MASTER rev 1.0: все версии
B650E AORUS TACHYON rev 1.0: все версии
B650I AORUS ULTRA rev 1.0: все версии
B650M AORUS ELITE AX rev 1.x: все версии
B650M AORUS ELITE rev 1.0: все версии
B650M AORUS PRO AX rev 1.x: все версии
B650M C rev 1.0: все версии
B650M DS3H rev 1.0: все версии
B650M GAMING X AX rev 1.x: все версии
B650M K rev 1.0: все версии
B660 AORUS ELITE AX DDR4 rev 1.0: все версии
B660 AORUS ELITE DDR4 rev 1.0: все версии

B660 AORUS MASTER DDR4 rev 1.0: все версии
B660 AORUS MASTER DDR4 rev 1.x: все версии
B660 AORUS MASTER rev 1.x: все версии
B660 DS3H AC DDR4 rev 1.0: все версии
B660 DS3H AC DDR4 rev 1.0/1.2: все версии
B660 DS3H AC DDR4 rev 1.1: все версии
B660 DS3H AC rev 1.0: все версии
B660 DS3H AX DDR4 rev 1.0: все версии
B660 DS3H AX DDR4 rev 1.0/1.1: все версии
B660 DS3H DDR4 rev 1.0: все версии
B660 DS3H DDR4 rev 1.0/1.1: все версии
B660 GAMING X AX DDR4 rev 1.0: все версии
B660 GAMING X DDR4 rev 1.0: все версии
B660 GAMING X rev 1.0: все версии
B660I AORUS PRO DDR4 rev 1.x: все версии
B660M AORUS ELITE AX DDR4 rev 1.0: все версии
B660M AORUS ELITE AX DDR4 rev 1.x: все версии
B660M AORUS ELITE DDR4 rev 1.0: все версии
B660M AORUS ELITE DDR4 rev 1.x: все версии
B660M AORUS PRO AX DDR4 rev 1.x: все версии
B660M AORUS PRO AX rev 1.x: все версии
B660M AORUS PRO DDR4 rev 1.0: все версии
B660M AORUS PRO rev 1.0: все версии
B660M D2H DDR4 rev 1.0: все версии
B660M D3H DDR4 rev 1.0: все версии
B660M DS3H AX DDR4 rev 1.x: все версии
B660M DS3H DDR4 rev 1.0: все версии
B660M GAMING AC DDR4 rev 1.0: все версии
B660M GAMING AC DDR4 rev 1.x: все версии
B660M GAMING AC rev 1.0: все версии
B660M GAMING DDR4 rev 1.0: все версии
B660M GAMING X AX DDR4 rev 1.x: все версии
B660M GAMING X AX rev 1.0: все версии
B660M GAMING X DDR4 rev 1.0: все версии

B660M GAMING X DDR4 rev 1.x: все версии
B660M GAMING X rev 1.0: все версии
B660M POWER DDR4 rev 1.0: все версии
B760M POWER rev 1.0: все версии
GA B560M D3P rev 1.0: все версии
H510M K rev 1.0: все версии
H510M K rev 1.1: все версии
H510M S2 rev 1.0/1.1/1.2: все версии
H510M S2 rev 1.3: все версии
H510M S2H rev 1.0: все версии
H510M S2H V2 rev 1.0: все версии
H510M S2H V2 rev 1.1: все версии
H510M S2H V2 rev 1.3: все версии
H510M S2P rev 1.0: все версии
H510M S2P rev 1.0 12: все версии
H610I DDR4 rev 1.0: все версии
H610M H DDR4 rev 1.0: все версии
H610M H DDR4 rev 1.1: все версии
H610M H DDR4 rev 1.1/1.3: все версии
H610M H DDR4 rev 1.2: все версии
H610M H rev 1.0: все версии
H610M H V2 DDR4 rev 1.0: все версии
H610M HD3P rev 1.0: все версии
H610M HD3P rev 20: все версии
H610M K DDR4 rev 1.0: все версии
H610M S2 DDR4 rev 1.0: все версии
H610M S2 DDR4 rev 1.1: все версии
H610M S2 DDR4 rev 1.1/1.3: все версии
H610M S2 DDR4 rev 1.2: все версии
H610M S2 rev 1.0: все версии
H610M S2 V2 DDR4 rev 1.0: все версии
H610M S2H DDR4 rev 1.0: все версии
H610M S2H DDR4 rev 1.1: все версии
H610M S2H DDR4 rev 1.1/1.3: все версии

H610M S2H DDR4 rev 1.2: все версии
H610M S2H rev 1.0: все версии
H610M S2H V2 DDR4 rev 1.0: все версии
N4120I H rev 1.0: все версии
N5105I H rev 1.0: все версии
Q670M D3H DDR4 rev 1.0: все версии
W480M VISION W rev 1.0: все версии
X570S AORUS ELITE AX rev 1.1: все версии
X570S AORUS ELITE rev 1.0: все версии
X570S AORUS MASTER rev 1.0: все версии
X570S AORUS PRO AX rev 1.0: все версии
X570S AORUS PRO AX rev 1.1: все версии
X570S GAMING X rev 1.0: все версии
X570S UD rev 1.0: все версии
X570SI AORUS PRO AX rev 1.0: все версии
X570SI AORUS PRO AX rev 1.1: все версии
X670 AORUS ELITE AX rev 1.0: все версии
X670 AORUS ELITE AX rev 1.1: все версии
X670 GAMING X AX rev 1.0: все версии
X670E AORUS MASTER rev 1.0: все версии
X670E AORUS XTREME rev 1.0: все версии
Z590 AORUS ELITE AX rev 1.0: все версии
Z590 AORUS ELITE rev 1.0: все версии
Z590 AORUS MASTER rev 1.0: все версии
Z590 AORUS PRO AX rev 1.0: все версии
Z590 AORUS TACHYON rev 1.0: все версии
Z590 AORUS ULTRA rev 1.0: все версии
Z590 D rev 1.0: все версии
Z590 GAMING X rev 1.x: все версии
Z590 UD AC rev 1.x: все версии
Z590 UD rev 1.0: все версии
Z590I AORUS ULTRA rev 1.0: все версии
Z690 AERO D rev 1.0: все версии
Z690 AERO D rev 1.x: все версии

Z690 AERO G DDR4 rev 1.0: все версии
Z690 AERO G DDR4 rev 1.x: все версии
Z690 AERO G rev 1.0: все версии
Z690 AERO G rev 1.x: все версии
Z690 AORUS ELITE AX DDR4 rev 1.0: все версии
Z690 AORUS ELITE AX DDR4 rev 1.x: все версии
Z690 AORUS ELITE AX DDR4 V2 rev 1.0: все версии
Z690 AORUS ELITE AX rev 1.0: все версии
Z690 AORUS ELITE AX rev 1.4: все версии
Z690 AORUS ELITE AX rev 1.x: все версии
Z690 AORUS ELITE DDR4 rev 1.0: все версии
Z690 AORUS ELITE DDR4 rev 1.x: все версии
Z690 AORUS ELITE DDR4 V2 rev 1.0: все версии
Z690 AORUS ELITE rev 1.0: все версии
Z690 AORUS ELITE STEALTH rev 1.0: все версии
Z690 AORUS MASTER rev 1.0: все версии
Z690 AORUS MASTER rev 1.x: все версии
Z690 AORUS PRO DDR4 rev 1.0: все версии
Z690 AORUS PRO DDR4 rev 1.x: все версии
Z690 AORUS PRO rev 1.0: все версии
Z690 AORUS PRO rev 1.x: все версии
Z690 AORUS TACHYON rev 1.0: все версии
Z690 AORUS ULTRA rev 1.0: все версии
Z690 AORUS ULTRA rev 1.x: все версии
Z690 AORUS XTREME rev 1.0: все версии
Z690 AORUS XTREME WATERFORCE rev 1.0: все версии
Z690 GAMING X DDR4 rev 1.0: все версии
Z690 GAMING X DDR4 rev 1.1: все версии
Z690 GAMING X DDR4 V2 rev 1.0: все версии
Z690 GAMING X rev 1.0: все версии
Z690 GAMING X rev 1.0/1.1: все версии
Z690 UD AC rev 1.0: все версии
Z690 UD AX DDR4 rev 1.0: все версии
Z690 UD AX DDR4 rev 1.x: все версии

Z690 UD AX DDR4 V2 rev 1.0: все версии
Z690 UD AX rev 1.0: все версии
Z690 UD AX rev 1.x: все версии
Z690 UD DDR4 rev 1.0: все версии
Z690 UD DDR4 rev 1.x: все версии
Z690 UD DDR4 V2 rev 1.0: все версии
Z690 UD rev 1.0: все версии
Z690 UD rev 1.x: все версии
Z690I AORUS ULTRA DDR4 rev 1.0: все версии
Z690I AORUS ULTRA LITE DDR4 rev 1.0: все версии
Z690I AORUS ULTRA LITE rev 1.0: все версии
Z690I AORUS ULTRA PLUS DDR4 rev 1.0: все версии
Z690I AORUS ULTRA PLUS rev 1.0: все версии
Z690I AORUS ULTRA rev 1.0: все версии
Z690M AORUS ELITE AX DDR4 rev 1.0: все версии
Z690M AORUS ELITE AX DDR4 rev 1.x: все версии
Z690M AORUS ELITE DDR4 rev 1.0: все версии
Z690M DS3H DDR4 rev 1.0: все версии
Z790 AERO G rev 1.0: все версии
Z790 AORUS ELITE AX DDR4 rev 1.0: все версии
Z790 AORUS ELITE AX rev 1.0: все версии
Z790 AORUS ELITE AX rev 1.1: все версии
Z790 AORUS ELITE DDR4 rev 1.0: все версии
Z790 AORUS ELITE rev 1.0: все версии
Z790 AORUS ELITE rev 1.1: все версии
Z790 AORUS MASTER rev 1.0: все версии
Z790 AORUS TACHYON rev 1.0: все версии
Z790 AORUS XTREME rev 1.0: все версии
Z790 D DDR4 rev 1.0: все версии
Z790 GAMING X AX rev 1.0: все версии
Z790 GAMING X AX rev 1.x: все версии
Z790 GAMING X rev 1.0: все версии
Z790 UD AC rev 1.0: все версии
Z790 UD AX rev 1.0: все версии

Z790 UD rev 1.0: все версии
Z790I AORUS ULTRA rev 1.0: все версии
Z790M AORUS ELITE AX rev 1.0: все версии
Z790M AORUS ELITE rev 1.0: все версии
UEFI firmware: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-01 / 2023-06-01

Ссылки на источник:

- <http://eclipsium.com/blog/supply-chain-risk-from-gigabyte-app-center-backdoor/>

Краткое описание: Выполнение произвольного кода в D-Link DAP-1360, DAP-2020

Идентификатор уязвимости: CVE-2023-32136

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: D-Link DAP-1360, DAP-2020:
до 6.15EUb01 Beta Hotfix (D-Link DAP-1360)
до 1.03rc004 Beta Hotfix (D-Link DAP-2020)

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-04 / 2023-05-04

Ссылки на источник:

- <https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10324>
- <https://www.zerodayinitiative.com/advisories/ZDI-CAN-18414/>
- <https://bdu.fstec.ru/vul/2023-02382>

Краткое описание: Обход безопасности в D-Link DIR-890L

Идентификатор уязвимости: CVE-2023-30063

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: D-Link DIR-890L: FW1.10 A1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Обход безопасности

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:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-01 / 2023-05-05

Ссылки на источник:

- https://github.com/Zarathustra-L/IoT_Vul/tree/main/D-Link/DIR-890L/Auth%20bypass
- <https://nvd.nist.gov/vuln/detail/CVE-2023-30063>
- <https://bdu.fstec.ru/vul/2023-02392>

Краткое описание: Обход безопасности в D-Link DIR-879

Идентификатор уязвимости: CVE-2023-30061

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: D-Link DIR-879: v105A1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Обход безопасности

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:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-01 / 2023-05-05

Ссылки на источник:

- <https://bdu.fstec.ru/vul/2023-02429>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-30061>
- https://github.com/Zarathustra-L/IoT_Vul/tree/main/D-Link/DIR-879

Краткое описание: Выполнение произвольного кода в Tenda AC23

Идентификатор уязвимости: CVE-2023-2649

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

Уязвимый продукт: Tenda AC23: 16.03.07.45_cn

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-11 / 2023-06-19

Ссылки на источник:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-2649>

Краткое описание: Отказ в обслуживании в Tenda AC18

Идентификатор уязвимости: CVE-2023-30135

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

Уязвимый продукт: Tenda AC18: V15.03.05.19(6318_)_cn

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

6 **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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-04 / 2023-05-11

Ссылки на источник:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-30135>

Краткое описание: Обход безопасности в D-Link DIR-868L A1

Идентификатор уязвимости: CVE-2023-29856

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: D-Link DIR-868L A1: 1.12

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Обход безопасности

7 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-02 / 2023-05-10

Ссылки на источник:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-29856>
- <https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10325>