



НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200423.5 | 23 апреля 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в маршрутизаторах D-Link

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	DSL-2875AL и DSL-2877AL ПО до v1.00.05
Дата выявления	19 марта 2020 г.
Дата обновления	25 марта 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2019-15655	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить несанкционированный доступ к данным посредством отправки специально созданного запроса к панели веб-администрирования. Уязвимость обусловлена хранением аутентификационных данных в открытом виде.</p> <p>CVSSv3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C CWE-522: Недостаточно надежная защита учетных данных</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	7.5

MITRE: CVE-2019-15656	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить несанкционированный доступ к данным. Уязвимость обусловлена передачей параметров «username_v» и «password_v» в открытом виде.</p> <p>CVSSv3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C CWE-312: Хранение критичных данных в незашифрованном виде</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	7.5
Ссылки на источники	<p>https://www.trustwave.com/en-us/resources/security-resources/security-advisories/?fid=26165 https://nvd.nist.gov/vuln/detail/CVE-2019-15655 https://nvd.nist.gov/vuln/detail/CVE-2019-15656 https://www.dlink.com/en/security-bulletin</p>	