НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200117.1 | 17 января 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Выполнение произвольных команд в ПО маршрутизатора D-Link DIR-601

Идентификатор уязвимости	MITRE: CVE-2019-16327
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять произвольные команды в целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена отсутствием проверки подлинности пользователя на стороне сервера.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Dlink DIR 601
Рекомендации по устранению	Производитель предлагает не использовать данную модель устройства
Дата выявления	24 декабря 2019 г.
Дата обновления	8 января 2020 г.
Оценка критичности уязвимости (CVSSv3)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)

Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Концептуальное подтверждение (P)
Наличие средств устранения уязвимости (RL)	Недоступно (U)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2019-16327 https://0x62626262.wordpress.com/2019/12/24/dlink-dir-601-router-authentication-bypass-and-csrf/