НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200318.5| 18 марта 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Уязвимость ПО маршрутизаторов D-link DIR-842

Идентификатор уязвимости	MITRE: CVE-2020-8962
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать сбой HTTPD-сервиса и выполнить произвольный код на целевом устройстве путем отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной обработкой входных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	D-Link DIR-842 REVC: ПО версии v3.13B09 HOTFIX
Рекомендации по устранению	Обновить программное обеспечение.
Дата выявления	13 февраля 2020 г.
Дата обновления	18 февраля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://ctrsec.io/index.php/2020/02/12/cve-2020-8962-d-link-dir-842-stack-based-buffer-overflow/