

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ
VULN-20190808.8 | 8 августа 2019 г.

Уровень опасности: **ВЫСОКИЙ**

Интъекция произвольного кода в маршрутизаторах D-Link DIR-818LW

Идентификатор уязвимости	MITRE: CVE-2019-12786
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного POST-запроса с вложенным вредоносным XML-документом. Уязвимость обусловлена отсутствием проверки вводимых данных в поле "IPAddress".
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимые системы и программное обеспечение	D-Link DIR-818LW с прошивкой v2.05.B03 до v2.06B01 BETA
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	10 июня 2019 г.
Дата обновления	11 июня 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Не требуется (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)

Функциональная версия (F)

Наличие средств устранения уязвимости (RL)

Официальное решение (O)

Достоверность сведений об уязвимости (RC)

Сведения подтверждены (C)

Ссылки

<https://github.com/TeamSerious/pocs/blob/master/iot/dlink/dir818-protected.pdf>

<https://nvd.nist.gov/vuln/detail/CVE-2019-12786>