НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210414.10 | 14 апреля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд оболочки в D-Link DIR-3060

Идентификатор уязвимости	MITRE: CVE-2021-28144
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (Внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды оболочки с root-привилегиями в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	DIR-3060: до версии 1.11b04 HF2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 марта 2021 г.
Дата обновления	15 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/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)	Низкий (L)
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://www.cybersecurity-help.cz/vdb/SB2021031512 https://packetstormsecurity.com/files/161757/D-Link-DIR-3060-1.11b04-Command-Injection.html https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10208 https://www.iot-inspector.com/blog/advisory-d-link-dir-3060/