НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191224.2 | 24 декабря 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в D-Link DCS-960L

Идентификатор уязвимости	MITRE: CVE-2019-17146 ZDI-19-1031 ZDI-CAN-8458
Идентификатор программной ошибки	CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному не аутентифицированному злоумышленнику выполнять произвольный код в целевом устройстве посредством отправки специально созданного SOAP-запроса на уязвимую IP-камеру. Уязвимость обусловлена некорректной обработкой заголовка запроса SOAP службой HNAP.
Категория уязвимого продукта	Периферийное оборудование
Уязвимое ПО	D-Link DCS-960L: v1.07.102
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	23 декабря 2019 г.
Дата обновления	23 декабря 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Смежная сеть (A)
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)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)

Ссылки на источники	https://www.zerodayinitiative.com/advisories/ZDI-19-1031/ https://www.cybersecurity-help.cz/vdb/SB2019122308