НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210922.3 | 22 сентября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в продуктах Hikvision

Идентификатор уязвимости	MITRE: CVE-2021-36260
Идентификатор программной ошибки	CWE: Не определен
Описание уязвимости	Уязвимость позволяет удаленному злоумышленнику получить доступ к целевой системе с правами суперпользователя посредством отправки специально сформированного вредоносного запроса к встроенному веб-серверу продуктов Hikvision. Уязвимость обусловлена некорректной фильтрацией входных данных.
Категория уязвимого продукта	IoT-устройства
Уязвимый продукт	Версии сборок до 210625: DS-2CVxxx1 DS-2CVxxx5 DS-2CVxxx6 HWI-xxxx IPC-xxxx DS-2CD1xx1 DS-2CD1x23 DS-2CD1x43(B) DS-2CD1x43(C) DS-2CD1x43G0E DS-2CD1x53(B) DS-2CD1x53(C) DS-2CD1xx7G0 DS-2CD2xx6G2 DS-2CD2xx7G2 DS-2CD2xx2WD DS-2CD2x21G0 DS-2CD2xx3G2 DS-2CD3xx6G2

DS-2CD3xx7G2
DS-2CD3xx7G0E
DS-2CD3x21G0
DS-2CD3x51G0
DS-2CD3xx3G2
DS-2CD4xx0
DS-2CD4xx6
DS-2CD5xx7
DS-2CD5xx5
iDS-2XM6810
iDS-2CD6810
DS-2XE62x7FWD(D)
DS-2XE30x6FWD(B)
DS-2XE60x6FWD(B)
DS-2XE62x2F(D)
DS-2XC66x5G0
DS-2XE64x2F(B)
DS-2CD7xx6G0
DS-2CD8Cx6G0
KBA18(C)-83x6FWD
(i)DS-2DExxxx
(i)DS-2PTxxxx
(i)DS-2SE7xxxx
DS-2DYHxxxx
DS-DY9xxxx
PTZ-Nxxxx
HWP-Nxxxx
DS-2DF5xxxx
DS-2DF6xxxx
DS-2DF6xxxx-Cx
DS-2DF7xxxx
DS-2DF8xxxx
DS-2DF9xxxx
iDS-2PT9xxxx
iDS-2SK7xxxx
iDS-2SK8xxxx
iDS-2SR8xxxx
iDS-2VSxxxx

Версии сборок до 210702:

DS-2TBxxx
DS-Bxxxx
DS-2TDxxxxB
DS-2TD1xxx-xx
DS-2TD2xxx-xx

	DS-2TD41xx-xx/Wx DS-2TD62xx-xx/Wx DS-2TD81xx-xx/Wx DS-2TD4xxx-xx/V2 DS-2TD62xx-xx/V2 DS-2TD81xx-xx/V2 V4.30.210 сборка 201224 - V4.31.000 сборка 210511: DS-76xxNI-K1xx DS-76xxNI-Qxx DS-HiLookI-NVR-1xxMHxx DS-HiLookI-NVR-2xxMHxx DS-HiWatchI-HWN-41xxMHxx DS-HiWatchI-HWN-42xxMHxx V4.30.300 сборка 210221 - V4.31.100 сборка 210511: DS-71xxNI-Q1xx DS-HiLookI-NVR-1xxMHxx DS-HiLookI-NVR-1xxHxx DS-HiWatchI-HWN-21xxMHxx DS-HiWatchI-HWN-21xxHxx
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 сентября 2021 г.
Дата обновления	19 сентября 2021 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	Концептуальное подтверждение

Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/ https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html