НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200319.6 | 19 марта 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ПО компании Huawei

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	V500R001C30, V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100
Дата выявления (обновления)	12 февраля 2020 г. (19 февраля 2020 г.)

Идентификаторы		Описание уязвимости, ссылки на источники	Оценка CVSSv3.1
Уязвимость	Программная ошибка		
MITRE: CVE-2020-1827; CVE-2020-1829; CVE-2020-1858; CVE-2020-1881	CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов); CWE-404: Некорректное освобождение ресурсов; CWE-415: Двойное освобождение	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать сбои в функционировании целевого устройства и его модулей путем отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным управлением ресурсами во время обработки данных. Рекомендации по устранению: обновить программное обеспечение	7.5

MITRE: CVE-2020-1873	CWE-125: Чтение за пределами буфера	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать перезагрузку целевого устройства путем отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной проверкой входных данных. Рекомендации по устранению: обновить программное обеспечение	7.5

Ссылки на источники	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-ipsec-en https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-02-resource-en https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-01-outofboundread-en