НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200313.1 | 13 марта 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Несанкционированный доступ к информации в ПО компании Huawei

Идентификатор уязвимости	MITRE: CVE-2020-1856
Идентификатор программной ошибки	CWE-200: Разглашение информации
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить несанкционированный доступ к информации в целевой системе посредством отправки специально сформированных команд управления.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Huawei NGFW, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600 и USG9500 версий V500R001C30, V500R001C60 и V500R005C00
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	17 февраля 2020 г.
Дата обновления	20 февраля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
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)	Отсутствует (N)
Влияние на доступность (A)	Отсутствует (N)

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.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en