НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200706.11 | 6 июля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Обход аутентификации в оборудовании Huawei

Идентификатор уязвимости	MITRE: CVE-2020-9099
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить несанкционированный доступ к целевой системе посредством отправки специально сформированных команд управления. Уязвимость обусловлена некорректной работой механизма аутентификации.
Категория уязвимого продукта	Средства защиты информации
Уязвимое ПО	Модуль IPS и NGFW продуктов Huawei: NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 с версиями ПО V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	11 июня 2020 г.
Дата обновления	8 июня 2020 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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-9099 https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200506-02-authentication-en