НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200907.1| 7 сентября 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в продуктах в Cisco ENCS серии 5400-W и CSP серии 5000-W

Идентификатор уязвимости	MITRE: CVE-2020-3446
Идентификатор программной ошибки	CWE-798: Использование жестко закодированных учетных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к интерфейсу командной строки уязвимого устройства с правами администратора посредством отправки специально созданных вредоносных сетевых пакетов. Уязвимость обусловлена наличием учетных записей пользователей со статическими паролями по умолчанию.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco ENCS серии 5400-W и CSP 5000-W работающие под управлением Cisco vWAAS с NFVIS до v6.4.5
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 августа 2020 г.
Дата обновления	19 августа 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-waas-encsw-cspw-cred-hZzL29A7