НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200617.3| 17 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Обход аутентификации в Cisco Adaptive Security Appliance

Идентификатор уязвимости	MITRE: CVE-2020-3125
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить полный доступ к целевой системы посредством отправки специально сформированного вредоносного ответа от центра распространения ключей (KDC) Kerberos. Уязвимость обусловлена некорректной проверкой подлинности ответов от сервера KDC.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco Adaptive Security Appliance (ASA) v9.6, 9.7, 9.8, 9.9, 9.10, 9.12, 9.13.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	6 мая 2020 г.
Дата обновления	7 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
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-2020-3125 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-asa-kerberos-bypass-96Gghe2sS