НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200706.1 | 6 июля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в ПО Cisco IOS и Cisco IOS XE

Идентификатор уязвимости	MITRE: CVE-2020-3230
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании модуля IKEv2 целевой системы посредством отправки специально сформированных сетевых пакетов IKEv2 SA-Init. Уязвимость обусловлена некорректной проверкой предоставленных пользователем данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco IOS 15.8(3)M2a Cisco IOS XE 16.12.1y
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	3 июня 2020 г.
Дата обновления	9 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/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)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)

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/2020-3230 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ikev2-9p23Jj2a