НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200715.2| 15 июля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в ПО Cisco IOS и Cisco IOS XE

Идентификатор уязвимости	MITRE: CVE-2020-3200 BDU:2020-02754
Идентификатор программной ошибки	CWE-371 Уязвимости, связанные с состоянием
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного вредоносного сетевого пакета, вызывающего состояние ошибки. Уязвимость обусловлена некорректным управлением состояния сервера SSH.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco IOS включая v15.2(1)S1 и Cisco IOS XE включая v16.12.1y
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	3 июня 2020 г.
Дата обновления	10 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
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/CVE-2020-3200 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssh-dos-Un22sd2A