НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200706.2| 6 июля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в ПО Cisco IOS

Идентификатор уязвимости	MITRE: CVE-2020-3199 CVE-2020-3257
Идентификатор программной ошибки	CWE-20 Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети вызвать отказ в обслуживании или выполнить произвольный код в целевой системе посредством отправки специально сформированных вредоносных сетевых пакетов. Уязвимость обусловлена некорректной проверкой входных данных в компоненте Cisco IOx.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco IOS 15.9 для маршрутизаторов Cisco 809, 829 и 1000 серии
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	3 июня 2020 г.
Дата обновления	11 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.1 AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
Вектор атаки (AV)	Смежная сеть (A)
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)	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-2020-3257 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-gos-vuln-s9qS8kYL