НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201106.3| 6 ноября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Запуск неподписанных приложений в Cisco IOS XR

Идентификатор уязвимости	MITRE: CVE-2020-3284
Идентификатор программной ошибки	CWE-284: Некорректное управление доступом
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику запустить не подписанное вредоносное приложение на целевом устройстве посредством подмены приложения на PXE сервере, или выдав себя за легитимный PXE сервер. Уязвимость обусловлена некорректной проверкой цифровой подписи загружаемых приложений с PXE сервера.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco IOS XR до v 6.5.2 для Cisco ASR 9000 Cisco IOS XR до v 7.1.1 для Cisco NCS 1000 Cisco IOS XR до v 7.2.1 для Cisco NCS 540 Cisco IOS XR до v 6.6.3, 6.6.25 и 7.0.2 для Cisco NCS 560 Cisco IOS XR до v 7.2.1 для Cisco NCS 5000 Cisco IOS XR до v 6.6.3 и 6.6.25 для Cisco NCS 5500
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	4 ноября 2020 г.
Дата обновления	4 ноября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.3 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)	Высокий (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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pxe-unsign-code-exec-qAa78fD2