НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190806.7 | 6 августа 2019 г.

Уровень опасности: ВЫСОКИЙ

Повышение привилегий в Cisco Application Policy Infrastructure Controller (APIC)

Идентификатор уязвимости	MITRE: CVE-2019-1889 CISCO: cisco-sa-20190703-ccapic-restapi BDU: 2019-02537
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику с привилегиями администратора повысить свои привилегии до уровня root посредством загрузки ВПО с помощью REST API. Уязвимость обусловлена отсутствием проверки пути загружаемого файла.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимые системы и программное обеспечение	Cisco APIC до v4.1(2g)
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	4 июля 2019 г.
Дата обновления	15 июля 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.2 AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Высокий (H)
Необходимость взаимодействия с пользователем (UI)	Не требуется (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 (E)	Не определено (X)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки	https://nvd.nist.gov/vuln/detail/CVE-2019-1889 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-ccapic-restapi