НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190808.3 | 8 августа 2019 г.

Уровень опасности: СРЕДНИЙ

Выполнение кода в Cisco Advanced Malware Protection (AMP)

Идентификатор уязвимости	MITRE: CVE-2019-1932 CISCO: cisco-sa-20190703-amp-commandinj BDU: 2019-02546
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику с правами администратора выполнить произвольный код с привилегиями службы AMP посредством размещения вредоносного файла в определенной директории файловой системы Windows. Уязвимость обусловлена недостаточной проверкой динамически загружаемых модулей уязвимого ПО.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимые системы и программное обеспечение	Cisco AMP for Endpoints для Windows включая v6.2.3.10807_030519
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 июля 2019 г.
Дата обновления	15 июля 2019 г.
Оценка критичности уязвимости (CVSSv3)	6.7 AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C
Вектор атаки (AV)	Локальный (L)
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-2019-1932 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-amp-commandinj