НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190808.2 | 8 августа 2019 г.

Уровень опасности: ВЫСОКИЙ

Выход за пределы защищенной оболочки в Cisco Unified Communications Domain Manager (Cisco Unified CDM)

Идентификатор уязвимости	MITRE: CVE-2019-1911 CISCO: cisco-sa-20190703-cucdm-rsh BDU: 2019-02545
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольные команды за пределами защищенной оболочки посредством ввода в интерфейс командной строки специально сформированной команды. Уязвимость обусловлена недостаточной проверкой вводимых пользователем данных в командную оболочку уязвимого ПО.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимые системы и программное обеспечение	Cisco Unified CDM включая v11.5 (3) PB3
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 июля 2019 г.
Дата обновления	17 июля 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.8 AV:L/AC:L/PR:L/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)	Низкий (L)
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://www.securityfocus.com/bid/109051 https://nvd.nist.gov/vuln/detail/CVE-2019-1911 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-cucdm-rsh