НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191212.4 | 12 декабря 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости веб-интерфейса управления ПО Cisco Firepower Management Center

Идентификатор уязвимости	MITRE: CVE-2019-12679, CVE-2019-12686 Cisco: cisco-sa-20191002-fmc-sql-inj BDU: 2019-03520, 2019-03527
Идентификатор программной ошибки	CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольный SQL-код на целевом устройстве путем отправки специально сформированных SQL-запросов. Уязвимость обусловлена некорректной проверкой вводимых данных
Категория уязвимого продукта	Средства защиты информации
Уязвимое ПО	Cisco FMC: Версии ПО до 6.2.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	2 октября 2019 г.
Дата обновления	9 октября 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
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 (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-sql-inj