НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200207.9 | 7 февраля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Уязвимость в веб-интерфейсе ПО Cisco Firepower Management Center

Идентификатор уязвимости	MITRE: CVE-2019-16028 CISCO: cisco-sa-20200122-fmc-auth
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации и выполнить произвольные действия от имени администратора в целевой системе посредством отправки вредоносных HTTP-запросов на целевое устройство. Уязвимость обусловлена некорректной обработкой ответов аутентификации облегченного протокола доступа к каталогам (LDAP) от внешнего сервера аутентификации.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco FMC до v.6.2.3, 6.4.0.7, и 6.5.0.2.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 января 2020
Дата обновления	22 января 2020
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/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)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Не требуется (N)

Масштаб последствий эксплуатации уязвимости (S)	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-20200122-fmc-auth