НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200512.4| 12 мая 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Наличие неизменяемых данных в ПО Cisco Firepower Management Center и Firepower User Agent

Идентификатор уязвимости	MITRE: CVE-2020-3318 CVE-2020-3301 CISCO: cisco-sa-fmcua-statcred-weeCcZct
Идентификатор программной ошибки	CWE-789: Неконтролируемое выделение памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ с привилегиями администратора к уязвимой части целевой системы. Уязвимость обусловлена наличием статического пароля для учетной записи с высоким уровнем привилегий.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco Firepower Management Center до v6.5.0 Cisco Firepower User Agent до v2.5.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	6 мая 2020 г.
Дата обновления	8 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
Необходимый уровень привилегий (PR)	Отсутствует (N)
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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-3318 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmcua-statcred-weeCcZct