НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201027.7 | 27 октября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ПО Cisco FMC

Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	ПО Cisco FMC до v6.6.1
Дата выявления	21 октября 2020 г.
Дата обновления	21 октября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-3499	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально созданных вредоносных запросов. Уязвимость обусловлена некорректной обработкой значений системных ресурсов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-399: Уязвимости, связанные с управлением ресурсами Рекомендации по устранению: обновить программное обеспечение.	8.6

MITRE: CVE-2020-3410	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе с помощью действующей карты общего доступа (CAC). Уязвимость обусловлена некорректной работой механизма аутентификации. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-287: Некорректная аутентификация Рекомендации по устранению: обновить программное обеспечение.	8.1

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftdfmc-dos-NjYvDcLA https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cacauthbyp-NCLGZm3Q