НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210827.2 | 27 августа 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Несанкционированный доступ в Cisco Application Policy Infrastructure Controller

Идентификатор уязвимости	MITRE: CVE-2021-1577
Идентификатор программной ошибки	CWE-284: Некорректное управление доступом
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД на чтение и запись файлов в целевой системе посредством загрузки специально сформированного файла. Уязвимость обусловлена некорректным управлением доступом.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Application Policy Infrastructure Controller: 3.2, 4.0, 4.1, 4.2, 5.0, 5.1 Cisco Cloud Application Policy Infrastructure Controller: 3.2, 4.0, 4.1, 4.2, 5.0, 5.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	26 августа 2021 г.
Дата обновления	26 августа 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
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)	Отсутствует (N)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021082610 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-frw-Nt3RYxR2