НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211008.2 | 8 октября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco AsyncOS for Web Security Appliances

Идентификатор уязвимости	MITRE: CVE-2021-34698
Идентификатор программной ошибки	CWE-401: Некорректное освобождение памяти до удаления последней ссылки (утечка памяти)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе. Уязвимость обусловлена утечкой памяти в прокси службе.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco AsyncOS for Web Security Appliances: 12.0, 12.5, 14.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	7 октября 2021 г.
Дата обновления	7 октября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
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)	Изменяется (C)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)
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://www.cybersecurity-help.cz/vdb/SB2021100701 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk