НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190806.8 | 6 августа 2019 г.

Уровень опасности: СРЕДНИЙ

Обход фильтров устройства защиты Cisco Email Security Appliance (ESA)

Идентификатор уязвимости	MITRE: CVE-2019-1844 CISCO: cisco-sa-20190501-esa-bypass BDU: 2019-02538
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти механизмы фильтрации сетевых пакетов уязвимого устройства посредством отправки сетевого пакета без указания информации в поле Content-Disposition на целевое устройство. Уязвимость обусловлена некорректным определением содержимого сетевых пакетов на уязвимом устройстве.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимые системы и программное обеспечение	Cisco Email Security Appliance (ESA) v11.1.0-131
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 марта 2019 г.
Дата обновления	5 июня 2019 г.
Оценка критичности уязвимости (CVSSv3)	5.3 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:X/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)	Не изменяется (U)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Низкое (L)

Влияние на доступность (A)	Отсутствует (N)
Степень зрелости доступных средств эксплуатации (E)	Не определено (X)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки	https://nvd.nist.gov/vuln/detail/CVE-2019-1844 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-esa-bypass http://www.securityfocus.com/bid/108149