

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191129.1 | 29 ноября 2019 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Отказ обслуживания в ПО компании Cisco

Идентификатор уязвимости	MITRE: CVE-2019-12673 Cisco: cisco-sa-20191002-asa-dos BDU: 2019-03533
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки вредоносных FTP-пакетов. Уязвимость обусловлена некорректной работой механизма проверки FTP-пакетов.
Категория уязвимого продукта	Средства защиты информации
Уязвимое ПО	Cisco Adaptive Security Appliance Software 9.10 Cisco Adaptive Security Appliance Software 9.12 Cisco Adaptive Security Appliance Software 9.4 Cisco Adaptive Security Appliance Software 9.5 Cisco Adaptive Security Appliance Software 9.6 Cisco Adaptive Security Appliance Software 9.7 Cisco Adaptive Security Appliance Software 9.8 Cisco Adaptive Security Appliance Software 9.9 Cisco Firepower Threat Defense Software 6.1.0 Cisco Firepower Threat Defense Software 6.2.0 Cisco Firepower Threat Defense Software 6.2.1 Cisco Firepower Threat Defense Software 6.2.2 Cisco Firepower Threat Defense Software 6.2.3 Cisco Firepower Threat Defense Software 6.3.0 Cisco Firepower Threat Defense Software 6.4.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	2 октября 2019 г.

Дата обновления	9 октября 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.4 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/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)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2019-12673 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-dos