

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191212.3 | 12 декабря 2019 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Уязвимости Multi-instance Container ПО Cisco Firepower Threat Defense

Идентификатор уязвимости	MITRE: CVE-2019-15240, CVE-2019-15252 Cisco: cisco-sa-20191016-spa-rce BDU: 2019-03669, 2019-03681
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному злоумышленнику, находящемуся в смежной сети, выполнить произвольный код с повышением привилегий на целевом устройстве путем ввода специально сформированных данных в веб-интерфейс. Уязвимость обусловлена некорректной проверкой данных пользовательского ввода.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco SPA112 2-Port Phone Adapter версия ПО до 1.4.1 SR4 Cisco SPA122 ATA with Router версия ПО до 1.4.1 SR4 Cisco ATA 190 Analog Telephone Adapter версия ПО до 1.2.2 SR1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 октября 2019 г.
Дата обновления	18 октября 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Смежная сеть (A)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)

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)	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)
<hr/>	
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-spa-rce