НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190813.1 | 13 августа 2019 г.

Уровень опасности: КРИТИЧЕСКИЙ

Загрузка произвольный файлов в коммутаторах Cisco Small Business

Идентификатор уязвимости	MITRE: CVE-2019-1912 CISCO: cisco-sa-20190806-sb220-auth_bypass
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику загружать произвольные файлы на целевое устройство посредством отправки специально сформированных HTTP(S)-пакетов. Уязвимость обусловлена неполной проверкой авторизации в веб-интерфейсе приложения.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимые системы и программное обеспечение	Коммутаторы Cisco Small Business серии 220 с ПО до v1.1.4.4 с включенным веб-интерфейсом управления.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	6 августа 2019 г.
Дата обновления	7 августа 2019 г.
Оценка критичности уязвимости (CVSSv3)	9.3 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H/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)	Высокое (H)
Влияние на доступность (A)	Высокое (H)

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://www.securitylab.ru/news/500339.php https://nvd.nist.gov/vuln/detail/CVE-2019-1912 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-auth_bypass