

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ
VULN-20190823.2 | 23 августа 2019 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Уязвимость в веб-интерфейсах различного ПО компании Cisco

Идентификатор уязвимости	MITRE: CVE-2019-1974
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к целевой системе с привилегиями администратора посредством отправки серии вредоносных запросов. Уязвимость обусловлена некорректной проверкой заголовка запроса в процессе аутентификации.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Cisco IMC Supervisor с v2.1 до v2.2.0.6 Cisco UCS Director с v5.5.0.0 до v6.7.2.0 Cisco UCS Director Express for Big Data с v2.1.0.0 и v3.7.2.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	21 августа 2019 г.
Дата обновления	21 августа 2019 г.
Оценка критичности уязвимости (CVSSv3)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/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)	Не требуется (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)

Ссылки на источники

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-authbypass>
<https://threatpost.com/cisco-patches-six-critical-bugs/147585/>