# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220305.1 | 5 марта 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

## Выполнение произвольного кода в Cisco IOS and Cisco IOS XE

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2017-6736<br>CVE-2017-6737<br>CVE-2017-6738<br>CVE-2017-6739<br>CVE-2017-6740<br>CVE-2017-6741<br>CVE-2017-6742<br>CVE-2017-6743<br>CVE-2017-6744 |
| Идентификатор программной ошибки | CWE-120: Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера) |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного SNMP-пакета через IPv4 или IPv6. Уязвимость обусловлена некорректной проверкой входных данных. |
| Категория уязвимого продукта | Серверное программное обеспечение и его компоненты |
| Уязвимый продукт | Cisco IOS: 15.6.3 M1 - 16.5.1<br>Cisco IOS XE: 3.16.1aS |
| Рекомендации по устранению | Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. |

| | |
|---|---|
| Дата выявления | 03 июля 2017 г. |
| Дата обновления | 03 июля 2017 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:H |
| Вектор атаки (AV) | Сетевой (N) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Низкий (L) |
| Необходимость взаимодействия с пользователем (UI) | Отсутствует (N) |
| Масштаб последствий эксплуатации уязвимости (S) | Изменяется (C) |
| Влияние на конфиденциальность (C) | Высокое (H) |
| Влияние на целостность (I) | Высокое (H) |
| Влияние на доступность (A) | Высокое (H) |
| Степень зрелости доступных средств эксплуатации | Высокая |
| Наличие средств устранения уязвимости | Официальное решение |
| Достоверность сведений об уязвимости | Сведения подтверждены |
| Ссылки на источники | https://www.cybersecurity-help.cz/vdb/SB2017070303<br>http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp |