# НКЦКИ

**НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ**

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

**УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ**

**VULN-20200921.4| 21 сентября 2020 г.**

**Уровень опасности: ВЫСОКИЙ**

**Наличие обновления: ЕСТЬ**

## Повышение привилегий в коммутаторах Cisco Nexus серии 3000 и 9000

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2020-3394 |
| Идентификатор программной ошибки | CWE-285: Некорректная авторизация |
| Описание уязвимости | Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством выполнения команды enable в функции Enable Secret. |
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимый продукт | Коммутаторы Nexus серии 3000<br>Коммутаторы Nexus серии 9000 в автономном режиме NX-OS |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 26 августа 2020 г. |
| Дата обновления | 26 августа 2020 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| Вектор атаки (AV) | Локальный (L) |
| 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 | Наличие не подтверждено |

| | |
|---|---|
| Наличие средств устранения уязвимости | Официальное решение |
| Достоверность сведений об уязвимости | Сведения подтверждены |
| Ссылки на источники | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n3n9k-priv-escal-3QhXJBC<br>https://www.cybersecurity-help.cz/vdb/SB2020082713 |