НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211108.3 | 8 ноября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Catalyst PON Switch CGP-ONT-1P

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Catalyst PON Switch CGP-ONT-1P : до 1.1.1.14 Catalyst PON Switch CGP-ONT-4P : до 1.1.3.17 Catalyst PON Switch CGP-ONT-4PV : до 1.1.3.17 Catalyst PON Switch CGP-ONT-4PVC : до 1.1.3.17 Catalyst PON Switch CGP-ONT-4TVCW : до 1.1.3.17
Дата выявления	4 ноября 2021 г.
Дата обновления	4 ноября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-34795	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена наличием отладочной учетной записи на устройстве со статическим паролем по умолчанию. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-798: Использование жестко закодированных учетных данных Рекомендации по устранению: обновить программное обеспечение	9.8

MITRE: CVE-2021-40112	Эксплуатация уязвимости позволяет удаленному злоумышленнику изменить конфигурацию целевого устройства посредством отправки специально сформированного HTTPS-запроса в веб-интерфейс управления. Уязвимость обусловлена некорректной поверкой HTTPS-запросов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C CWE-288: Обход аутентификации, связанный с альтернативными путями или каналами Рекомендации по устранению: обновить программное обеспечение	9.1
MITRE: CVE-2021-40113	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды от имени пользователя root в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-77: Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд) Рекомендации по устранению: обновить программное обеспечение	9.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021110417 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr