НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201007.6 | 7 октября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco IOS XR

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco IOS XR, v5.0.0 – v7.2.1
Дата выявления	2 сентябрь 2020 г.
Дата обновления	2 сентябрь 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-3530	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику вызвать отказ в обслуживании уязвимого оборудования посредством выполнения специально сформированной команды. Уязвимость обусловлена некорректным разграничением привилегий групп пользователей на выполнение определенных команд. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H/E:U/RL:O/RC:C CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение.	8.4

MITRE: CVE-2020-3473	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику получить административный доступ к уязвимому оборудованию посредством выполнения специально сформированной команды. Уязвимость обусловлена некорректным разграничением привилегий групп пользователей на выполнение определенных команд. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение.	7.8

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-cli-privescl-sDVEmhqv https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-LJtNFjeN