НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211125.3 | 25 ноября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Expressway

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Expressway: X14.0.4, X14.1
Дата выявления	24 ноября 2021 г.
Дата обновления	24 ноября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-34798	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена ошибкой разыменования указателя NULL. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-476: Разыменование нулевого указателя Рекомендации по устранению: обновить программное обеспечение	7.5

MITRE: CVE-2021-36160	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректным граничным условием. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE: CVE-2021-40438	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N/E:P/RL:O/RC:C CWE-918: Подделка запроса со стороны сервера Рекомендации по устранению: обновить программное обеспечение	9.3

Ссылки на источники	http://lists.apache.org/thread.html/re4162adc051c1a0a79e7a24093f3776373e8733abaff57253fef341d@%3Ccvs.httpd.apache.org%3E http://httpd.apache.org/security/vulnerabilities_24.html https://www.cybersecurity-help.cz/vdb/SB2021091706 http://lists.apache.org/thread.html/ree7519d71415ecdd170ff1889cab552d71758d2ba2904a17ded21a70@%3Ccvs.httpd.apache.org%3E https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-httpd-2.4.49-VWL69sWQ