НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211115.3 | 15 ноября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Apache Traffic Control

Идентификатор уязвимости	MITRE: CVE-2021-43350
Идентификатор программной ошибки	CWE-90: Некорректная нейтрализация специальных элементов, используемых в LDAP-запросах (внедрение LDAP)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированного POST запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке имен пользователей в Apache Traffic Control Traffic Ops.
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	Apache Traffic Control: 5.0.0, 5.1.0, 5.1.1, 5.1.2, 5.1.3, 6.0.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 ноября 2021 г.
Дата обновления	12 ноября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
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://www.cybersecurity-help.cz/vdb/SB2021111211 http://trafficcontrol.apache.org/security/ http://www.openwall.com/lists/oss-security/2021/11/11/4 http://www.openwall.com/lists/oss-security/2021/11/11/3