НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210921.1 | 21 сентября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Apache HTTP Server

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Apache HTTP Server: 2.4.0, 2.4.0.0, 2.4.0.1, 2.4.0.2, 2.4.0.3, 2.4.0.4, 2.4.0.5, 2.4.0.6, 2.4.0.7, 2.4.1, 2.4.2, 2.4.3, 2.4.4, 2.4.5, 2.4.6, 2.4.7, 2.4.8, 2.4.9, 2.4.10, 2.4.11, 2.4.12, 2.4.13, 2.4.14, 2.4.15, 2.4.16, 2.4.17, 2.4.18, 2.4.19, 2.4.20, 2.4.21, 2.4.22, 2.4.23, 2.4.24, 2.4.25, 2.4.26, 2.4.27, 2.4.28, 2.4.29, 2.4.32, 2.4.33, 2.4.34, 2.4.35, 2.4.36, 2.4.37, 2.4.38, 2.4.39, 2.4.40, 2.4.41, 2.4.42, 2.4.43, 2.4.44, 2.4.45, 2.4.46, 2.4.47, 2.4.48
Дата выявления	17 сентября 2021 г.
Дата обновления	17 сентября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-34798	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе 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 в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена ошибкой границ памяти в модуле mod_proxy_uwsg. 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 выполнить SSRF-атаку посредством отправки специально. сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных в модуле mod_proxy. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N/E:U/RL:O/RC:C CWE-918: Подделка запроса со стороны сервера Рекомендации по устранению: обновить программное обеспечение	9.3

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021091706