НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210727.1 | 27 июля 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

NTLM relay атака на Active Directory Certificate Services (AD CS)

Идентификатор уязвимости	Не определен
Идентификатор программной ошибки	CWE-294: Обход аутентификации при помощи перехвата и воспроизведения
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации и получить несанкционированный доступ к системе посредством выполнения атаки типа NTLM relay. Уязвимость обусловлена слабостью аутентификации в NTLM.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Windows Server: 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2019 20H2, 2019 1709, 2019 1803, 2019 1903, 2019 1909, 2019 2004
Рекомендации по устранению	Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами
Дата выявления	24 июля 2021 г.
Дата обновления	24 июля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
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)	Отсутствует (N)
Степень зрелости доступных средств эксплуатации	Функциональная версия
Наличие средств устранения уязвимости	Обходной путь
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021072402 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV210003 https://github.com/topotam/PetitPotam