НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200813.5| 13 августа 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Получение аутентификационных данных в TeamViewer Desktop для Windows

Идентификатор уязвимости	MITRE: CVE-2020-13699
Идентификатор программной ошибки	CWE-428: Отсутствие кавычек вокруг элемента в пути поиска
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить NTLM-хэш текущего пользователя Windows и НСД к данным в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректными ограничениями пользовательских обработчиков URI в TeamViewer Desktop для Windows.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	TeamViewer до v15.8.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	29 июля 2020 г.
Дата обновления	29 июля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/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)	Требуется (R)
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	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020081024 https://www.helpnetsecurity.com/2020/08/06/cve-2020-13699/ https://nvd.nist.gov/vuln/detail/CVE-2020-13699