

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200914.8 | 14 сентября 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Повышение привилегий в ОС Windows

Идентификатор уязвимости	MITRE: CVE-2020-1115
Идентификатор программной ошибки	CWE-122: Переполнение буфера в динамической памяти
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством запуска специально созданного вредоносного приложения. Уязвимость обусловлена некорректной обработкой драйвером CLFS объектов в памяти.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Windows: 7, 8.1, RT 8.1, 10 Windows Server: 2008, 2012, 2016, 2019, v1903, v1909, v2004
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 сентября 2020 г.
Дата обновления	8 сентября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
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://talosintelligence.com/vulnerability_reports/TALOS-2020-1098
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1115>