НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190912.1 | 12 сентября 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Переполнение буфера в ОС Windows

Идентификатор уязвимости	MITRE: CVE-2019-1215
Идентификатор программной ошибки	CWE-119: Некорректное ограничение выполняемых операций в пределах буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе с привилегиями администратора посредством запуска специального созданного вредоносного приложения. Уязвимость обусловлена некорректной обработкой объектов памяти.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Windows: 7, 8.1, 10, 10 1607, 10 1703, 10 1709, 10 1803, 10 1809, 10 1903, RT 8.1 Windows Server: 1803, 1903, 2008, 2008 R2, 2012, 2012 R2, 2016, 2019
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	10 сентября 2019 г.
Дата обновления	10 сентября 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Не требуется (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 (E)	Концептуальное подтверждение (P)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1215 https://www.cybersecurity-help.cz/vdb/SB2019091019?affChecked=1