НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191213.2 | 13 декабря 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость компонента Win32k в ОС Windows

Идентификатор уязвимости	MITRE: CVE-2019-1458
Идентификатор программной ошибки	CWE-269: Некорректное управление привилегиями
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в режиме ядра в целевой системе посредством запуска специально созданного вредоносного приложения. Уязвимость обусловлена некорректной обработкой объектов в памяти компонентом Win32k.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Windows 10 x32/x64 Windows 10 Version 1607 x32/x64 Windows 7 for SP 1 x32/x64 Windows 8.1 x32/x64 Windows RT 8.1 Windows Server 2008 SP 2 x32/x64 Windows Server 2008 SP 2 x32/x64 (Server Core installation) Windows Server 2008 for Itanium-Based Systems SP 2 Windows Server 2008 R2 for Itanium-Based Systems SP 1 Windows Server 2008 R2 for x64-based Systems SP 1 Windows Server 2008 R2 for x64-based Systems SP 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation)

Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	10 декабря 2019 г.
Дата обновления	11 декабря 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:U/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)	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)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Наличие не подтверждено (U)
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-2019-1458 https://nvd.nist.gov/vuln/detail/CVE-2019-1458