НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191113.3 | 13 ноября 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в Microsoft Windows

Идентификатор уязвимости	MITRE: CVE-2019-1441
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе убедив пользователя открыть специально созданный вредоносный документ или посетить специально созданный вредоносный веб-ресурс. Уязвимость обусловлена некорректной работой библиотеки шрифтов Windows при обработке встроенных шрифтов.
Категория уязвимого продукта	Операционные системы Windows и их компоненты
Уязвимое ПО	Microsoft Windows 7 sp1, Microsoft Windows Server 2008 sp2, Microsoft Windows Server 2008 r2 sp1.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 ноября 2019 г.
Дата обновления	13 ноября 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
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 (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://nvd.nist.gov/vuln/detail/CVE-2019-1441 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1441 https://www.zerodayinitiative.com/advisories/ZDI-19-985/