# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191217.1 | 17 декабря 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Уязвимость библиотеки шрифтов в ОС Windows

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2019-1468 |
| Идентификатор программной ошибки | CWE-20: Некорректная проверка входных данных |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному неаутентифицированному злоумышленнику выполнить код в целевой системе с привилегиями текущего пользователя в результате посещения им специально созданной веб-страницы или открытия специально созданного документа. Уязвимость обусловлена некорректной обработкой встроенных шрифтов компонентом Win32k Graphics. |
| Категория уязвимого продукта | Операционные системы Microsoft и их компоненты |
| Уязвимое ПО | Windows 10 x32/x64<br>Windows 10 Version 1607 x32/x64<br>Windows 10 Version 1709 x32/x64/ARM64<br>Windows 10 Version 1803 x32/x64/ARM64<br>Windows 10 Version 1809 x32/x64/ARM64<br>Windows 10 Version 1903 x32/x64/ARM64<br>Windows 10 Version 1909 x32/x64/ARM64<br>Windows 7 SP 1 x32/x64<br>Windows 8.1 x32/x64<br>Windows RT 8.1<br>Windows Server 2008 SP 2 x32/x64<br>Windows Server 2008 SP 2 x32/x64 (Server Core installation)<br>Windows Server 2008 for Itanium-Based Systems SP 2<br>Windows Server 2008 R2 for Itanium-Based Systems SP 1<br>Windows Server 2008 R2 for x64-based Systems SP 1<br>Windows Server 2008 R2 for x64-based Systems SP 1 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2012 (Server Core installation) |

| | |
|---|---|
| | Windows Server 2012 R2<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2019 (Server Core installation)<br>Windows Server, version 1803 (Server Core Installation)<br>Windows Server, version 1903 (Server Core installation)<br>Windows Server, version 1909 (Server Core installation) |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 10 декабря 2019 г. |
| Дата обновления | 13 декабря 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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1468<br>https://nvd.nist.gov/vuln/detail/CVE-2019-1468 |