НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191227.1 | 27 декабря 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в ОС Windows

Идентификатор уязвимости	MITRE: CVE-2019-1184 ZDI-19-706
Идентификатор программной ошибки	CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить привилегии в целевой системе посредством запуска в ней специально созданного приложения. Уязвимость обусловлена некорректной работой процесса регистрации COM-объектов.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Windows 10 Version 1803 x32/x64/ARM64 Windows 10 Version 1809 x32/x64/ARM64 Windows 10 Version 1903 x32/x64/ARM64 Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server, version 1803 (Server Core Installation) Windows Server, version 1903 (Server Core installation)
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	14 августа 2019 г.
Дата обновления	19 августа 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-2019-1184 https://nvd.nist.gov/vuln/detail/CVE-2019-1184 https://www.thezdi.com/blog/2019/12/19/privilege-escalation-via-the-core-shell-com-registrar-object https://www.zerodayinitiative.com/advisories/ZDI-19-706/