НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190816.2 | 16 августа 2019 г.

Уровень опасности: ВЫСОКИЙ

Повышение привилегий в ОС Windows

Идентификатор уязвимости	MITRE: CVE-2019-1162
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена неправильной обработкой вызовов Advanced Local Process Call.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Windows 10 для x64/32-разрядных систем Windows 10 Version 1607 для x64/32-разрядных систем Windows 10 Version 1703 для x64/32-разрядных систем Windows 10 Version 1709 для 64/32-разрядных систем Windows 10 Version 1709 для ARM 64-разрядных систем Windows 10 Version 1803 для ARM 64-разрядных систем Windows 10 Version 1803 для x64/32-разрядных систем Windows 10 Version 1809 для ARM 64-разрядных систем Windows 10 Version 1809 для x64/32-разрядных систем Windows 10 Version 1903 для ARM 64-разрядных систем Windows 10 Version 1903 для x64/32-разрядных систем Windows 7 для x64/32-разрядных систем Service Pack 1 Windows 8.1 для x64/32-разрядных систем Windows RT 8.1 Windows Server 2008 R2 для Itanium-разрядных систем Service Pack 1 Windows Server 2008 R2 для x64-разрядных систем Service Pack 1 Windows Server 2012 Windows Server 2012 R2

	Windows Server 2016 Windows Server 2019 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	15 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)	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)	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-2019-1162