НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191122.1 | 22 ноября 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость компонента Windows Certificate Dialog ОС Windows

Идентификатор уязвимости	MITRE: CVE-2019-1388
Идентификатор программной ошибки	CWE-269: Некорректное управление привилегиями
Описание уязвимости	Эксплуатация уязвимости позволяет локальному авторизованному злоумышленнику повысить свои привилегии в целевой системе посредством использования специально созданного приложения. Уязвимость обусловлена некорректным применением привилегий к пользователю во время вызова компонента Windows Certificate Dialog.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Windows 10 V1607 Windows 10 V1709 Windows 10 V1803 Windows 10 V1809 Windows 10 V1903 Windows 7 Service Pack 1 Windows 8.1 Windows RT 8.1 Windows Server 2008 Service Pack 2 Windows Server 2008 Service Pack 2 (Server Core installation) Windows Server 2008 R2 Service Pack 1 Windows Server 2008 R2 Service Pack 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)

	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	12 ноября 2019 г.
Дата обновления	14 ноября 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://www.zerodayinitiative.com/advisories/ZDI-19-975/ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1388 https://threatpost.com/windows-uac-flaw-privilege-escalation/150463/