НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190814.4 | 14 августа 2019 г.

Уровень опасности: ВЫСОКИЙ

Удаленное выполнение кода в ОС Windows

Идентификатор уязвимости	MITRE: CVE-2019-1188
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить код в целевой системе с текущими привилегиями пользователя посредством специально созданных вредоносных файлов формата .LNK и связанного с ним двоичного файла. Уязвимость обусловлена некоренным анализом файла .LNK в проводнике Windows или любом другом приложении.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Windows: 10 1709, 10 1803, 10 1809, 10 1903 Windows Server: 1803, 1903, 2019
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	13 августа 2019 г.
Дата обновления	14 августа 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.5 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://www.cybersecurity-help.cz/vdb/SB2019081408 https://www.zdnet.com/article/microsoft-august-2019-patch-tuesday-fixes-93-security-bugs/ https://threatpost.com/wormable-remote-desktop-bugs-august-patch-tuesday/147302/ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1188