

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)  
E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200520.4 | 20 мая 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Повышение привилегий в диспетчере печати Windows

Идентификатор уязвимости	MITRE: CVE-2020-1048
Идентификатор программной ошибки	CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством запуска специально сформированного вредоносного файла. Уязвимость обусловлена некорректной работой службы диспетчера очереди печати Windows.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Windows: 7, 8.1, 10, 10 1607, 10 1709, 10 1803, 10 1809, 10 1903, 10 1909, RT 8.1 Windows Server: 1803, 1903, 1909, 2008, 2008 R2, 2012, 2012 R2, 2016, 2019
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 мая 2020 г.
Дата обновления	13 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
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	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены

---

Ссылки на источники

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1048>