

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20221110.18 | 10 ноября 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Microsoft Windows Print Spooler service

Идентификатор уязвимости	MITRE: CVE-2022-41073
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код с привилегиями «SYSTEM» в целевой системе посредством запуска специально созданной вредоносной программы. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Windows: 7 - 11 22H2 Windows Server: 2008 - 2022 20H2
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	8 ноября 2022 г.
Дата обновления	8 ноября 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.4 CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с	Отсутствует (N)

пользователем (UI)

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

Не определено

Наличие средств устранения уязвимости

Официальное решение

Достоверность сведений об уязвимости

Не определено

Ссылки на источники

<http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073>