НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200921.5| 21 сентября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Microsoft Windows Defender

Идентификатор уязвимости	MITRE: CVE-2020-1163 CVE-2020-1170
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 созданного вредоносного приложения. Уязвимость обусловлена некорректной политикой безопасности в Microsoft Windows Defender.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Windows Defender для Windows: 7, 8.1, RT 8.1, 10, 10 1511, 10 1607, 10 1703, Server 2008, Server 2012, Server 2016, Server 2019
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	6 сентября 2020 г.
Дата обновления	16 сентября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	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	Наличие не подтверждено
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-2020-1163 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1170 https://www.cybersecurity-help.cz/vdb/SB2020060936