НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200212.2 | 12 февраля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повреждение памяти в Windows Media Foundation

Идентификатор уязвимости	MITRE: CVE-2020-0738
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить полный доступ к целевой системе, убедив пользователя открыть специально созданный вредоносный документ или посетить вредоносную веб-страницу. Уязвимость обусловлена переполнением буфера памяти при обработке объектов.
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 R2, 2012, 2012 R2, 2016, 2019
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	11 февраля 2020 г.
Дата обновления	12 февраля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.9 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)	Концептуальное подтверждение (P)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0738