НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200615.3| 15 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Microsoft GDI+

Идентификатор уязвимости	MITRE: CVE-2020-1248
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена некорректной обработкой данных в памяти интерфейса графических устройств Windows (GDI).
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Windows: 10 1903, 10 1909, 10 2004 Windows Server, версия 1903 (установка Server Core) Windows Server, версия 1909 (установка Server Core) Windows Server, версия 2004 (установка Server Core)
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 июня 2020 г.
Дата обновления	9 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.6 AV:L/AC:L/PR:N/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)	Отсутствует (N)
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-2020-1248