НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200611.1 | 11 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Несанкционированный доступ к информации в Microsoft Windows

Идентификатор уязвимости	MITRE: CVE-2020-1206
Идентификатор программной ошибки	CWE-200: Разглашение информации
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к памяти ядра в целевой системе посредством отправки специально сформированного вредоносного сетевого пакета на сервер SMBv3 или при подключении SMB-клиента к вредоносному SMB-серверу. Уязвимость обусловлена некорректной обработкой SMB-запросов функцией компрессии.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Windows 10 Версия 1903 для 32-битных систем Windows 10 версии 1903 для систем на базе ARM64 Windows 10 Версия 1903 для 64-разрядных систем Windows 10 Версия 1909 для 32-битных систем Windows 10 версии 1909 для систем на базе ARM64 Windows 10 Версия 1909 для 64-разрядных систем Windows 10 Версия 2004 для 32-битных систем Windows 10 версии 2004 для систем на базе ARM64 Windows 10 Версия 2004 для 64-разрядных систем 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:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Отсутствует (N)
Влияние на доступность (A)	Отсутствует (N)
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-2020-1206 https://blog.zecops.com/vulnerabilities/smbleedingghost-writeup-chaining-smbleed-cve-2020-1206-with-smbghost/ https://thehackernews.com/2020/06/SMBleed-smb-vulnerability.html https://github.com/ZecOps/CVE-2020-1206-POC