cyberART

АНАЛИТИЧЕСКАЯ СПРАВКА

Уязвимость в протоколе Server Message Block 3.1.1 (SMBv3)

innoSTage
группа компаний

cyberART

ОГЛАВЛЕНИЕ

1. ОПИСАНИЕ УЯЗВИМОСТИ

В протоколе SMB 3.1.1 (SMBv3) обнаружена уязвимость удаленного выполнения кода (RCE-уязвимость) и присвоен идентификатор CVE-2020-0796 (на текущий момент технические детали уязвимости не опубликованы).

Уязвимость заключается в некорректном способе обработки соединений, использующих «сжатие», что позволяет злоумышленнику, не прошедшему проверку подлинности, отправить специально сформированный пакет на целевой сервер SMBv3 и выполнить произвольный код в уязвимой системе с привилегией «SYSTEM». Уязвимости подвержена как серверная, так и клиентская часть SMB.

На данный момент компанией Microsoft не выпущено обновления, закрывающего указанную уязвимость на хостах с ОС Windows. Также неизвестно существование эксплойтов использующих данную уязвимость.

2. ВЛИЯНИЕ

Злоумышленник может выполнить произвольный код с системными привилегиями на целевой системе двумя способами:

1) компрометация SMB-клиента: уязвимый хост подключается к уже скомпрометированному злоумышленником серверу по протоколу SMBv3;

2) компрометация SMB-сервера: злоумышленник отправляет специально сформированный сетевой пакет целевому SMBv3-серверу.

Данной уязвимости подвержены следующие версии ОС Windows:

- Windows 10 Version 1903 for 32-bit Systems
- Windows 10 Version 1903 for ARM64-based Systems
- Windows 10 Version 1903 for x64-based Systems
- Windows 10 Version 1909 for 32-bit Systems
- Windows 10 Version 1909 for ARM64-based Systems
- Windows 10 Version 1909 for x64-based Systems
- Windows Server, version 1903 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)

3. РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ УРОВНЯ ЗАЩИЩЁННОСТИ

1) Для временного решения проблемы на стороне SMB-сервера компания Microsoft рекомендует отключить функцию «сжатия» в протоколе SMBv3 с помощью команды PowerShell, приведенной ниже (после внесения изменений перезагрузка не требуется):

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 1 -Force

Запуск PowerShell должен выполняться от имени администратора.

Данное решение не предотвращает эксплуатацию уязвимости на SMB-клиентах.

2) Так же крайне рекомендуется установить обновления для этой уязвимости, как только они станут доступны.

3) При наличии опубликованных сетевых ресурсов по протоколу SMB на внешнем периметре рекомендуем рассмотреть возможность их закрытия (заблокировать порт 445/TCP).

ПРИЛОЖЕНИЕ

Дата публикации:	10.03.2020
Опасность:	Высокая
CVE ID:	CVE-2020-0796
Вектор эксплуатации:	Удалённое выполнение кода
Воздействие:	Компрометация системы
Наличие эксплойтов:	Нет данных
Уязвимые продукты:	ОС семейства Windows
Уязвимые протоколы:	SMB 3.1.1
Информация о уязвимости:	ADV200005
Решение:	До выхода обновления, исправляющего уязвимость, отключить функцию «сжатия» в протоколе SMB 3.1.1

КОНТАКТЫ

Адрес:
420015, Казань, ул. Подлужная, 60

Телефон: +7 (843) 567 42 90
E-mail: soc@cyberart.ru