Аналитический отчет по уязвимости PrintNightmare:

Исследователи из Sangfor опубликовали на GitHub техническое описание CVE-2021-1675, которая вытекает в CVE-2021-34527 -> CVE-2021-36958 -> CVE-2021-1678 и PoC в открытом доступе. Ошибку назвали PrintNightmare, представляет дырку в диспетчере очереди печати spoolsv.exe. По умолчанию Print Spooler включен на всех машинах, за исключением Windows Server Core.

Эксплуатация уязвимостей и риски: приводит к удаленному выполнению кода (RCE) и позволяет взять атакованную систему под полный контроль, с любого аутентифицированного пользователя. Уязвимость заключается в вызове RpcAddPrinterDriver диспетчера очереди печати Windows. Клиент использует вызов RPC для добавления драйвера на сервер, сохраняя нужный драйвер в локальном каталоге или на сервере через SMB. Затем клиент выделяет объект DRIVER_INFO_2 и инициализирует объект DRIVER_CONTAINER, который содержит выделенный объект DRIVER_INFO_2. Объект DRIVER_CONTAINER используется в вызове RpcAddPrinterDriver для загрузки драйвера. Драйвер может содержать произвольный код, который будет выполняться с правами SYSTEM на сервере - в службе диспетчера очереди печати. Позволяет заполучить учётные данные, проникать в систему для дальнейшего доступа к корпоративной сети и службам Microsoft. Можно устанавливать и удалять программы, просматривать и изменять файлы, а также создавать новые учётные записи с полными правами. Позволяет повышать локальные привилегий до SYSTEM, путем эксплуатации ошибки при включении политики "Point and Print Restrictions" и при выключенном уведомлении о запросе на повышение прав в параметре "When installing drivers for a new connection". Проверка разрешений при установке драйверов печати, позволяющей накатывать вредонос для удаленного выполнения кода или локального повышения привилегий в уязвимых системах, также устанавливать на свои устройства, подписанные драйвера доверенного сертификата Authenticod и устанавливающегося на любое другое сетевое устройство, на которое у него есть права администратора. Позволяет использовать «поворотное» устройство для получения привилегий SYSTEM на других устройствах, - установив вредоносный драйвер (LPE). Появляется Magniber, который удаляет загрузчик DLL, который вводится в процесс, а затем распаковывается для локального обхода файлов и шифрования файлов на скомпрометированном устройстве. TTP включает удаление резервных копий для предотвращения восстановления зашифрованных систем жертвами и обход средств защиты Windows для кражи учетных данных и повышения привилегий -Vice Society (MITM).

Методология атак: Использование таких утилит, как proxychains и impacket; Таргетинг резервных копий, для предотвращения восстановления системы; Ухудшение работы серверов ESXi; Использование DLL с PrintNightmare; Обход средств защиты Windows для кражи учетных данных и повышения прав.

Рекомендации:

Отрубить spoolsv.exe, особенно на контроллерах домена; Заблочить ссылку sso.umagnet.ru; отключить службу "Диспетчер очереди печати" через Power Shell; Отключить входящую удаленную печать через редактор локальной групповой политики; Настройка регистрации устройства в Microsoft Endpoint Manager; Управление группой Local Administrators; Добавление правил Microsoft Defender ASR для защиты от конкретных проблем безопасности; Следовать стандартным правилам безопасности Windows 10; Ограничить круг лиц с привилегиями локального администратора, использовать Microsoft Endpoint Manager и Microsoft Defender для обеспечения защиты облачного ПК; Установка доступа Azure AD для безопасной аутентификации, включая MFA, и снижения рисков при входе пользователя; Оптимальным является отключение защиты от CVE-2021-1678 до тех пор, пока Microsoft не выпустит новое руководство; Обновлением в ОС по умолчанию был активирован ключ реестра: [HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Control \ Print] «RpcAuthnLevelPrivacyEnabled» = двойное слово: 00000001, который используется для повышения уровня проверки подлинности RPC, используемого для сетевой печати.

Видео PoC: https://youtu.be/qU3vQ-B-FPY, https://youtu.be/m0LQvf07fjA, https://youtu.be/qU3vQ-B-FPY.
Референсы: https://github.com/afwu/PrintNightmare, https://github.com/byt3bl33d3r/ItWasAllADream.