Уязвимость в диспетчере печати Windows CVE-2021-34527 "PrintNightmare"

07.12.2021 07:54:59

Печать статьи FAQ

Категория:	Оборудование	**Голоса:**	0
Состояние:	общедоступное (всем)	**Результат:**	0.00 %
Язык:	ru	**Последнее обновление:**	09:06:27, Чтв 08 Июл, 2021 г.

Ключевые слова

PrintNightmare CVE-2021-34527 Уязвимость Remote Code Execution Vulnerability

Симптомы (общедоступное)

Проблема (общедоступное)

В диспетчере печати ОС Windows всех версий была обнаружена уязвимость, позволяющая злоумышленнику с учетной записью пользователя выполнять код на любом сервере\ПК. Так как диспетчер печати включен по умолчанию во всех клиентских и серверных версиях ОС Windows, ей подвержены практически все компьютеры с Windows.
Данная уязвимость должна быть закрыта разработчиком ПО - Microsoft. За ходом закрытия этой уязвимости можно следить по ссылке https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Решение (общедоступное)

Обновление 06.07 Компания Microsoft выпустила экстренное исправление KB5005010 для данной уязвимости для всех актуальных версий ОС (и Win7\2012R2, которые уже сняты с поддержки). После установки данного обновления пользователи без прав Администратора на сервере не будут иметь возможность установить не подписанный цифровой подписью драйвер. Так же в нем добавлен ключ HKEY_LOCAL_MACHINE \Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint\RestrictDriverInstallationToAdministrators (DWORD), который запрещает пользователям установку даже подписанных драйверов на сервере печати.

Вредоносный код добавляет DLL в директорию C:\Windows\System32\spool\drivers, которая в последствии используется для получения доступа к системе. Поэтому самым умеренным обходным решением (до выпуска патча от Microsoft), с точки зрения нарушения стандартных рабочих процессов пользователей и администраторов, является изменение прав доступа к директории (запрет для УЗ Системы\System на запись).
Это можно сделать, выполнив PS скрипт ниже:

```
$Path = "C:\Windows\System32\spool\drivers"

$Acl = (Get-Item $Path).GetAccessControl('Access')

$Ar = New-Object
System.Security.AccessControl.FileSystemAccessRule("System", "Modify",
"ContainerInherit, ObjectInherit", "None", "Deny")

$Acl.AddAccessRule($Ar)

Set-Acl $Path $Acl
```

После выполнения этого код Администраторы не смогут добавить новые драйвера в систему. В случае необходимости, можно откатить изменения, выполнив PS скрипт ниже:

```
$Path = "C:\Windows\System32\spool\drivers"

$Acl = (Get-Item $Path).GetAccessControl('Access')

$Ar = New-Object
System.Security.AccessControl.FileSystemAccessRule("System", "Modify",
"ContainerInherit, ObjectInherit", "None", "Deny")

$Acl.RemoveAccessRule($Ar)

Set-Acl $Path $Acl
```

Так как драйвера разных версий\производителей могут по разному реагировать на изменение прав доступа к директории, перед переносом этого обходного решения в продуктивную среду, его обязательно нужно протестировать для вашей инфраструктуры.