Microsoft Windows Print Spooler Vulnerability CVE-2021-34527

("PrintNightmare") Cybersecurity Update For Windows 7 OS

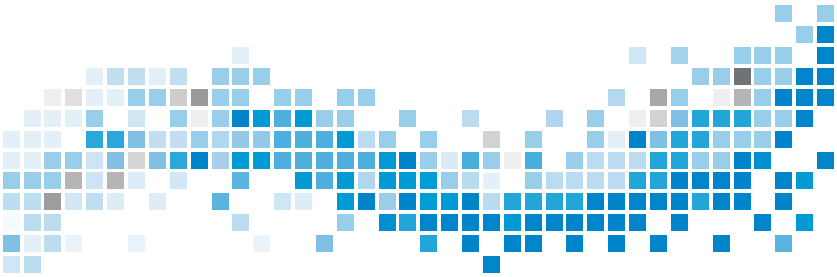

Table of Contents

Table of Contents

Microsoft Windows Print Spooler Vulnerability CVE-2021-34527

("PrintNightmare") Cybersecurity Update For Windows 7 OS

en-US ■ 9/24/2021

1 About the Update

PrintNightmare is a vulnerability affecting Microsoft Windows operating systems (OS).

A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.[1]

PrintNightmare does not affect safety and performance on any of the ZEISS devices.

However, ZEISS recommends updating devices with the Microsoft patch and/or registry settings, as applicable, to ensure continued cybersecurity. ZEISS has analyzed the impact of the vulnerability on ZEISS products running Windows OS and only devices listed below must run the update.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Disable the Printer Spooler Group Policy

It is recommended that a site IT Administrator performs this task.

1. Login to the instrument.
2. In the search box on the taskbar, type `gpedit.msc` to run the Group Policy editor.
3. Navigate to **Local Computer Policy > Computer Configuration > Administrative Templates > Printers**.
4. Select **Allow Print Spooler** to accept client connections.
5. Double-click the policy to open it.
6. Select **Disabled**.
7. Select **OK** to save the policy.
8. Restart the instrument.

Result

✓ Doing the above steps will block the remote attack vector by preventing inbound remote printing operations. The system will no longer function as a print server, but local printing to a directly attached device will still be possible.

[1] Microsoft website: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

✓ This Group Policy change will set the following registry key `HKEY_LOCAL_MACHINE\ Software\Policies \Microsoft\Windows NT\Printers\ Register-SpoolerRemoteRpcEndPoint = 2`

3 Deactivate Point and Print in the Windows Registry

We recommend an IT administrator to perform this task.

Action

1. Login to the instrument.
2. In the search box on the taskbar, type `regedit`, then select Registry Editor.
3. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE \Policies\Microsoft\Windows NT\Printers`.
4. If it exists, expand the Printers branch, and make sure that the PointandPrint group does not exist.
   NOTE! The Printers branch does not exist in the factory configuration.
   ⇨ If the **PointandPrint** group exists, check the following settings, if it exists then set the value to 0 .
   `NoWarningNoElevationOnInstall = 0 or does not exist`
   `UpdatePromptSettings = 0 or does not exist`
5. Restart the instrument.

الثغرة الأمنية في التخزين المؤقت للطباعة في Microsoft Windows CVE-2021-34527

تحديث الأمان عبر الإنترنت ("PrintNightmare") لنظام التشغيل Windows 7

الثغرة الأمنية في التخزين المؤقت للطباعة في Microsoft Windows
CVE-2021-34527

1 نبذة عن التحديث

PrintNightmare هي ثغرة أمنية تؤثر على أنظمة تشغيل Microsoft Windows (نظام التشغيل).

توجد ثغرة أمنية تنطوي على تنفيذ تعليمات برمجية عن بُعد عند قيام خدمة التخزين المؤقت لطباعة Windows بتنفيذ عمليات الملفات ذات الامتيازات بصورة غير صحيحة. بإمكان المهاجم الذي ينجح في استغلال هذه الثغرة الأمنية تشغيل تعليمات برمجية تحكمية بامتيازات SYSTEM. بإمكان المهاجم بعد ذلك تثبيت برامج، أو عرض بيانات أو تغييرها أو حذفها؛ أو إنشاء حسابات جديدة بحقوق المستخدم الكاملة.[2]

لا تؤثر PrintNightmare على سلامة وأداء أي من أجهزة ZEISS.

ولكن توصي ZEISS بتحديث الأجهزة باستخدام إعدادات تصحيح Microsoft و/أو إعدادات السجل، حسب الاقتضاء، لضمان استمرار الأمن عبر الإنترنت.
قامت ZEISS بتحليل تأثير الثغرة الأمنية على منتجات ZEISS التي تعمل بنظام التشغيل Windows ويجب على الأجهزة المسرودة أدناه فقط تشغيل التحديث.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 تعطيل نهج مجموعة التخزين المؤقت للطابعة

من المستحسن أن يقوم مسؤول تكنولوجيا المعلومات في الموقع بتنفيذ هذه المهمة.

طريقة

1. قم بتسجيل الدخول إلى الجهاز.
2. في مربع البحث على شريط المهام، اكتب `gpedit.msc` لتشغيل محرر نهج المجموعة.
3. انتقل إلى **نهج الكمبيوتر المحلي > تكوين الكمبيوتر > قوالب إدارية > الطابعات**.
4. حدد **السماح بالتخزين المؤقت للطباعة** لقبول اتصالات العملاء.
5. انقر نقرا مزدوجا فوق النهج لفتحه.
6. حدد **معطل**.
7. حدد **موافق** لحفظ النهج.
8. أعد تشغيل الجهاز.

نتيجة

✓ سيؤدي تنفيذ الخطوات المذكورة أعلاه إلى حظر متجه الهجوم البعيد عن طريق منع عمليات الطباعة عن بعد الواردة. لن يعمل النظام بعد الآن كخادم طباعة، ولكن ستظل الطباعة المحلية إلى جهاز متصل مباشرةً ممكنة.

[2] موقع الويب لشركة Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

الثغرة الأمنية في التخزين المؤقت للطباعة في Microsoft Windows
CVE-2021-34527

✓ سيؤدي هذا التغيير في نهج المجموعة إلى تعيين مفتاح التسجيل التالي `HKEY_LOCAL_MACHINE\ Software\Policies\Microsoft\Windows NT\Printers\RegisterSpoolerRemoteRpcEndPoint = 2`

3 إلغاء تنشيط Point and Print في سجل Windows

نوصي بقيام مسؤول تكنولوجيا المعلومات بتنفيذ هذه المهمة.

طريقة

1. قم بتسجيل الدخول إلى الجهاز.
2. في مربع البحث على شريط المهام، اكتب `regedit`، ثم حدد محرر السجل.
3. انتقل إلى `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\`.
4. إذا كان موجودًا، فقم بتوسيع فرع الطابعات وتأكد من أن مجموعة PointandPrint غير موجودة.
   ملاحظة! فرع الطابعات غير موجود في تكوين المصنع.
   ⇦ إذا كانت المجموعة **PointandPrint** موجودة، فتحقق من الإعدادات التالية، إذا كانت موجودة، ثم قم بتعيين القيمة على 0.
   `NoWarningNoElevationOnInstall = 0` أو غير موجود
   `UpdatePromptSettings = 0` أو غير موجود
5. أعد تشغيل الجهاز.

Уязвимост на спулера за отпечатване на Microsoft Windows CVE-2021-34527

(PrintNightmare) Актуализация на киберсигурността за ОС Windows 7

1 Относно актуализацията

PrintNightmare е уязвимост, засягаща операционните системи (ОС) Windows на Microsoft.

Уязвимост от отдалечено изпълнение на код съществува, когато услугата за спулер за отпечатване на Windows неправилно изпълнява привилегировани файлови операции. Нападател, който успешно е използвал тази уязвимост, може да изпълни произволен код със СИСТЕМНИ привилегии. След това нападателят може да инсталира програми, да преглежда, променя или изтрива данни или да създава нови акаунти с пълни потребителски права.[3]

PrintNightmare не засяга безопасността и производителността на което и да е от устройствата на ZEISS.

ZEISS обаче препоръчва актуализиране на устройствата с поправките и/или настройките на системния регистър на Microsoft, ако е приложимо, за да се гарантира непрекъсната киберсигурност. ZEISS анализира въздействието на уязвимостта върху своите продукти с ОС Windows, като само устройствата, посочени по-долу, трябва да бъдат актуализирани.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Деактивиране на груповите правила за спулера за принтери

Препоръчително е ИТ администраторът на обекта да извърши тази задача.

Начин на работа

1. Влезте в инструмента.
2. В полето за търсене на лентата на задачите напишете `gpedit.msc`, за да стартирате редактора на груповите правила.
3. Отидете до **Локални правила на компютъра > Компютърна конфигурация > Административни шаблони > Принтери**.
4. Изберете **Позволяване на спулер за отпечатване**, за да приемете клиентските връзки.
5. Щракнете двукратно върху правилото, за да го отворите.
6. Изберете **Деактивирано**.

[3] Уеб сайт на Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

7. Изберете **OK**, за да запазите правилото.
8. Рестартирайте инструмента.

Резултат

✓ Изпълняването на гореспоменатите стъпки ще блокира вектора за отдалечена атака чрез предотвратяване на входящите операции за отдалечено отпечатване. Системата вече няма да функционира като сървър за отпечатване, но локалното отпечатване на директно свързано устройство все още ще бъде възможно.

✓ Тази промяна в груповите правила ще зададе следния ключ от системния регистър `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\RegisterSpoolerRemoteRpcEndPoint = 2`

3 Деактивирайте Point and Print в системния регистър на Windows

Препоръчваме ИТ администраторът да извърши тази задача.

Начин на работа

1. Влезте в инструмента.
2. В полето за търсене на лентата на задачите напишете `regedit`, след което изберете редактора на системния регистър.
3. Отидете до `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Ако съществува, разширете клона на принтерите и се уверете, че групата PointandPrint не съществува.
   УКАЗАНИЕ! Клонът на принтерите не съществува във фабричната конфигурация.
   ⇨ Ако групата **PointandPrint** съществува, проверете следните настройки. Ако съществува, задайте стойността на 0.
   `NoWarningNoElevationOnInstall = 0 или не съществува`
   `UpdatePromptSettings = 0 или не съществува`
5. Рестартирайте инструмента.

Microsoft Windows Print Spooler 漏洞 CVE-2021-34527

（“PrintNightmare“）Windows 7 操作系统（OS）的网络安全更新

zh-CHS • 2021/9/24

1 关于更新

PrintNightmare 是影响 Microsoft Windows 操作系统（OS）的漏洞。

当 Windows Print Spooler 服务执行特权文件操作不当时，存在远程代码执行漏洞。 成功利用此漏洞的攻击者可以使用系统特权运行任意代码。 然后，攻击者可以安装程序; 查看、更改或删除数据; 或创建具有完全用户权的新帐户。[4]

PrintNightmare 不影响任何 ZEISS 设备的安全性和性能。

但是，ZEISS 建议根据适用情况，使用 Microsoft 修补程序和/或注册设置更新设备，以确保持续网络安全。 ZEISS 分析了该漏洞对运行 Windows操作系统（OS）的 ZEISS 产品的影响，只有下面列出的设备必须运行更新。

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 禁用 Printer Spooler 组政策

建议网站 IT 管理员执行此任务。

操作步骤

1. 登录到仪器。
2. 在任务栏上的搜索框中，键入 `gpedit.msc` 以运行该组政策编辑器。
3. 导航到**本地计算机政策 > 计算机配置 > 管理模板 > 打印机**。
4. 选择**允许 Print Spooler** 以接受客户端连接。
5. 双击该政策以打开它。
6. 选择**禁用**。
7. 选择**确定**以保存该政策。
8. 重新启动仪器。

结果

✓ 执行上述步骤将阻止远程攻击途径，防止入站远程打印操作。 系统将不再作为打印服务器运行，但直接连接设备的本地打印仍是可能的。

✓ 此组政策变更将设置以下注册表密码 `HKEY_LOCAL_MACHINE\ Software\Policies\Microsoft\Windows NT\Printers\RegisterSpoolerRemoteRpcEndPoint = 2`

[4] Microsoft **网站**： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

3 在 Windows 注册表中停用 Point and Print

我们建议 IT 管理员执行此任务。

操作步骤

1. 登录到仪器。
2. 在任务栏上的搜索框中，键入 `regedit`，然后选择注册表编辑器。
3. 导航到 `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`。
4. 如果它存在，请扩展打印机分支，并确保 PointandPrint 组不存在。
   提示！ 打印机分支在工厂配置中不存在。
   ⇨ 如果 **PointandPrint** 组存在，请检查以下设置，如果它存在，则将值设置为 0。
   `NoWarningNoElevationOnInstall = 0` 或不存在
   `UpdatePromptSettings = 0` 或不存在
5. 重新启动仪器。

Ranjivost usmjerivača ispisa u sustavu Microsoft Windows CVE-2021-34527

(„PrintNightmare”) Ažuriranje računalne sigurnosti za OS Windows 7

1 O ažuriranju

PrintNightmare je ranjivost koja utječe na operacijske sustave Microsoft Windows (OS).

Ranjivost pri daljinskom izvršavanju koda javlja se kada servis usmjerivača ispisa u sustavu Windows nepravilno izvede povlaštene operacije s datotekama. Napadač koji uspješno iskoristi tu ranjivost mogao bi pokrenuti nasumični kod s ovlastima na razini sustava. Napadač bi tada mogao instalirati programe, prikazati, promijeniti ili izbrisati podatke ili stvoriti nove račune s punim korisničkim pravima.[5]

PrintNightmare ne utječe na sigurnost i performanse ni na jednom uređaju ZEISS.

Međutim, ZEISS preporučuje ažuriranje uređaja Microsoftovim postavkama zakrpe i/ili registra, ovisno o potrebi, kako bi se osigurala kontinuirana računalna sigurnost. ZEISS je analizirao utjecaj ranjivosti na proizvode ZEISS s operacijskim sustavom Windows OS i samo uređaji navedeni u nastavku moraju pokrenuti ažuriranje.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Onemogućivanje pravila grupe za usmjerivač pisača

Preporučuje se da taj zadatak obavlja IT administrator.

Način postupanja

1. Prijavite se na instrument.
2. U okvir za pretraživanje na programskoj traci upišite `gpedit.msc` da biste pokrenuli uređivač pravila grupe.
3. Otiđite na **Pravila lokalnog računala > Konfiguracija računala > Administrativni predlošci > Pisači**.
4. Odaberite **Dopusti usmjerivaču ispisa** da prihvati klijentske veze.
5. Dvaput kliknite pravilo da biste ga otvorili.
6. Odaberite **Onemogućeno**.
7. Odaberite **U redu** da biste spremili pravilo.
8. Ponovno pokrenite instrument.

[5] Web-mjesto tvrtke Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Rezultat

✓ Gore navedeni koraci blokirat će vektor daljinskog napada sprječavanjem ulaznih operacija daljinskog ispisa. Sustav više neće funkcionirati kao poslužitelj za ispis, ali će lokalni ispis na izravno priključenom uređaju i dalje biti moguć.

✓ Ovom promjenom pravila grupe postavit će se sljedeći ključ registra `HKEY_LOCAL_MACHINE\ Software\Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Deaktiviranje značajke Point and Print u registru sustava Windows

Preporučujemo da taj zadatak obavlja IT administrator.

Način postupanja

1. Prijavite se na instrument.
2. U okvir za pretraživanje na programskoj traci upišite `regedit`, a zatim odaberite Uređivač registra.
3. Otiđite na `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Proširite granu Pisači ako postoji i uvjerite se da grupa PointandPrint ne postoji.
   NAPOMENA! Grana Pisači ne postoji u tvorničkoj konfiguraciji.
   ⇨ Ako grupa **PointandPrint** postoji, provjerite sljedeće postavke; ako postoji, postavite vrijednost na 0.
   `NoWarningNoElevationOnInstall = 0 ili ne postoji`
   `UpdatePromptSettings = 0 ili ne postoji`
5. Ponovno pokrenite instrument.

Chyba zabezpečení zařazovací služby tisku systému Microsoft Windows CVE-2021-34527

(„PrintNightmare“) Aktualizace ohledně kybernetické bezpečnosti pro operační systém Windows 7

cs ■ 24.09.2021

Chyba zabezpečení zařazovací služby tisku systému Microsoft Windows CVE-2021-34527

1 Informace o aktualizaci

PrintNightmare je chyba zabezpečení ovlivňující operační systémy Microsoft Windows.

Pokud služba zařazování tisku systému Windows nesprávně provede privilegované operace se soubory, může se projevit chyba zabezpečení umožňující vzdálené spuštění kódu. Útočník, který by tuto chybu zabezpečení úspěšně zneužil, by mohl spustit libovolný kód se systémovými oprávněními. Útočník by pak mohl instalovat programy, prohlížet, měnit nebo mazat data nebo vytvářet nové účty s plnými uživatelskými právy.[6]

PrintNightmare neovlivňuje bezpečnost a výkon na žádném ze zařízení ZEISS.

Společnost ZEISS nicméně pro zajištění trvalé kybernetické bezpečnosti doporučuje aktualizovat zařízení pomocí opravy společnosti Microsoft nebo registru. Společnost ZEISS analyzovala dopad této chyby zabezpečení na produkty ZEISS s operačním systémem Windows a aktualizaci je nutné provést pouze na níže uvedených zařízeních.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Zakázání zásad skupiny služby zařazování tisku

Doporučuje se, aby tento úkon provedl IT správce webu.

Postup

1. V přístroji se přihlaste.
2. Do vyhledávacího pole na hlavním panelu zadejte `gpedit.msc`, abyste spustili editor zásad skupiny.
3. Přejděte na **Zásady místního počítače > Konfigurace počítače > Šablony pro správu > Tiskárny**.
4. Vyberte možnost **Povolit zařazovací službě tisku přijímat připojení klienta**.
5. Otevřete zásadu dvojitým kliknutím.
6. Vyberte možnost **Zakázáno**.
7. Uložte zásadu výběrem položky **OK**.
8. Restartujte přístroj.

[6] Web společnosti Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Výsledek

- ✓ Provedením výše uvedených kroků zablokujete vektor vzdáleného útoku tím, že zabráníte příchozím vzdáleným tiskovým operacím. Systém již nebude fungovat jako tiskový server, místní tisk pomocí přímo připojeného zařízení bude ale stále možný.
- ✓ Tato změna zásad skupiny nastaví následující klíč registru `HKEY_LOCAL_MACHINE\ Software\Policies \Microsoft\Windows NT\Printers \RegisterSpoolerRemoteRpcEndPoint = 2`

3 Deaktivace funkce Ukázat a tisknout v registru systému Windows

Doporučuje se, aby tento úkon provedl IT správce webu.

Postup

1. V přístroji se přihlaste.
2. Do vyhledávacího pole na hlavním panelu zadejte `regedit` a pak vyberte Editor registru.
3. Přejděte na `HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows NT\Printers`.
4. Pokud existuje, rozbalte větev Printers a ujistěte se, že neexistuje skupina PointandPrint.
   UPOZORNĚNÍ! Větev Printers v tovární konfiguraci neexistuje.
   - ⇨ Pokud skupina **PointandPrint** existuje, zkontrolujte následující nastavení, pokud existuje, nastavte hodnotu na 0.
     `NoWarningNoElevationOnInstall = 0 nebo neexistuje`
     `UpdatePromptSettings = 0 nebo neexistuje`
5. Restartujte přístroj.

Sikkerhedsrisiko ved Microsoft Windows-printspooler CVE-2021-34527

("PrintNightmare") Cybersikkerhedsopdatering til Windows 7-operativsystemet

da ■ 24-09-2021

1 Om opdateringen

PrintNightmare er en sikkerhedsrisiko, der berører Microsoft Windows-operativsystemer (OS).

Der er en sikkerhedsrisiko i forbindelse med fjernkørsel af programkode, når tjenesten Windows-printspooler udfører filhandlinger med privilegerede filer på forkert vis. En person med ondsindede hensigter, der har held til at udnytte denne sikkerhedsrisiko, kan køre skadelig kode med SYSTEM-rettigheder. En person med ondsindede hensigter kan derefter installere programmer, få vist, ændre eller slette data eller oprette nye konti med komplette brugerrettigheder.[7]

PrintNightmare påvirker ikke sikkerheden og ydeevnen på nogen af ZEISS-enhederne.

ZEISS anbefaler dog, at enhederne opdateres med Microsoft-programrettelses- og/eller registreringsdatabaseindstillingerne, hvis det er relevant, for at sikre fortsat cybersikkerhed. ZEISS har analyseret indvirkningen af sikkerhedsrisikoen på ZEISS-produkter, der kører Windows-operativsystemet, og kun de enheder, der er angivet nedenfor, skal køre opdateringen.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Deaktiver gruppepolitik for printerspooler

Det anbefales, at denne opgave udføres af stedets it-administrator.

Fremgangsmåde

1. Log på instrumentet.
2. Skriv `gpedit.msc` i søgefeltet på proceslinjen for at køre redigeringsprogrammet til gruppepolitik.
3. Gå til **Lokal computerpolitik > Computerkonfiguration > Administrative skabeloner > Printere**.
4. Vælg **Tillad, at printspooleren** accepterer klientforbindelser.
5. Dobbeltklik på politikken for at åbne den.
6. Vælg **Deaktiveret**.
7. Vælg **OK** for at gemme politikken.
8. Genstart instrumentet.

[7] Microsoft-websted: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Resultat

- ✓ Hvis du udfører ovenstående trin, blokeres der for fjernangrebsvektoren ved at forhindre indgående fjernudskrivningshandlinger. Systemet fungerer ikke længere som en printerserver, men lokal udskrivning til en direkte tilsluttet enhed vil stadig være mulig.
- ✓ Denne ændring af gruppepolitikken angiver følgende registreringsdatabasenøgle `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Deaktiver pegning og udskrivning i Windows-registreringsdatabasen

Vi anbefaler, at denne opgave udføres af en it-administrator.

Fremgangsmåde

1. Log på instrumentet.
2. Skriv `regedit` i søgefeltet på proceslinjen, og vælg derefter Registreringseditor.
3. Gå til `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Hvis den findes, skal du udvide printerforgreningen og kontrollere, at gruppen PointandPrint (Peg og udskriv) ikke findes. **BEMÆRK! Printerforgreningen findes ikke i fabrikskonfigurationen.**
   - ⇨ Hvis gruppen **PointandPrint** (Peg og udskriv) findes, skal du kontrollere følgende indstillinger, og hvis den findes, skal værdien angives til 0.
     `NoWarningNoElevationOnInstall = 0 eller findes ikke`
     `UpdatePromptSettings = 0 eller findes ikke`
5. Genstart instrumentet.

Beveiligingslek in Microsoft Windows Print Spooler CVE-2021-34527

("PrintNightmare") Cyberbeveiligingsupdate voor Windows 7-besturingssysteem

nl ■ 24-9-2021

1 Over de update

PrintNightmare is een beveiligingslek in het besturingssysteem Microsoft Windows.

Er is een beveiligingslek dat het mogelijk maakt om op afstand code uit te voeren wanneer de Windows Print Spooler-service bepaalde geprivilegieerde bestandsbewerkingen niet op de juiste manier uitvoert. Een aanvaller die erin slaagt gebruik te maken van dit beveiligingslek, zou in staat zijn willekeurige code uit te voeren met SYSTEEM-rechten. De aanvaller kan dan programma's installeren, gegevens bekijken, wijzigen of verwijderen, of nieuwe accounts maken met volledige gebruikersrechten.[8]

PrintNightmare heeft geen gevolgen voor de veiligheid en prestaties op ZEISS-apparaten.

ZEISS beveelt echter aan de apparaten bij te werken met de Microsoft-patch en/of registerinstellingen, al naar gelang hetgeen van toepassing is, om de cyberbeveiliging zeker te stellen. ZEISS heeft de impact geanalyseerd van het beveiligingslek op ZEISS-producten waarop het Windows-besturingssysteem wordt gebruikt. Alleen op de hieronder genoemde apparaten moet de update worden uitgevoerd.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Het groepsbeleid voor de printerspooler uitschakelen

Aanbevolen wordt dat een IT-beheerder ter plaatse deze taak uitvoert.

Werkwijze

1. Log in op het instrument.
2. Typ in het zoekvak op de taakbalk `gpedit.msc` om de groepsbeleidseditor te openen.
3. Ga naar **Beleid voor lokale computer > Computerconfiguratie > Beheersjablonen > Printers**.
4. Selecteer **Toestaan dat de printerspooler clientverbindingen accepteert**.
5. Dubbelklik op het beleid om het te openen.
6. Selecteer **Uitgeschakeld**.

[8] Microsoft-website: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

7. Selecteer **OK** om het beleid op te slaan.
8. Start het instrument opnieuw op.

Resultaat

✓ De bovenstaande stappen blokkeren de externe aanvalsvector door inkomende externe afdrukopdrachten te blokkeren. Het systeem fungeert niet meer als printserver, maar lokaal afdrukken op een rechtstreeks aangesloten apparaat blijft mogelijk.

✓ Met deze wijziging in de groepsbeleideditor wordt de volgende registersleutel ingesteld: `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Point-and-print deactiveren in het Windows-register

We raden aan deze taak te laten uitvoeren door een IT-beheerder.

Werkwijze

1. Log in op het instrument.
2. Typ `regedit` in het zoekveld op de taakbalk en selecteer de Registereditor.
3. Ga naar `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Open de vertakking Printers als deze bestaat en controleer of de groep PointandPrint niet bestaat.
   OPMERKING! De vertakking Printers maakt geen deel uit van de fabrieksconfiguratie.

   ⇨ Als de groep **PointandPrint** bestaat, controleert u de volgende instellingen. Als de groep bestaat, stelt u de waarde in op 0.
   `NoWarningNoElevationOnInstall = 0 of bestaat niet`
   `UpdatePromptSettings = 0 of bestaat niet`
5. Start het instrument opnieuw op.

Microsoft Windowsi prindispuuleri haavatavus CVE-2021-34527

(„PrintNightmare“) Küberturvalisuse värskendus operatsioonisüsteemile Windows 7

et ■ 24.09.2021

1 Värskenduse teave

PrintNightmare on haavatavus, mis puudutab Microsoft Windowsi operatsioonisüsteeme (OS).

Koodi kaugtäitmine on haavatav, kui Windowsi prindispuuleri teenus teeb privilegeeritud failitoiminguid valesti. Seda haavatavust edukalt kasutanud ründajal oli võimalus käivitada suvaline kood koos SÜSTEEMI õigustega. Ründaja võib seejärel installida programme; vaadata, muuta või kustutada andmeid; või luua uusi täielike kasutajaõigustega kontosid.[9]

PrintNightmare ei mõjuta üheski ZEISS-seadmes ohutust ega jõudlust.

Siiski soovitab ZEISS küberturvalisuse kestvaks tagamiseks värskendada seadmeid Microsofti paiga- ja/või registrisätetega. ZEISS on analüüsinud haavatavuse mõju Windowsi OS-iga töötavatele ZEISS-i toodetele ja värskenduse peavad käivitama ainult allpool loetletud seadmed.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Printerispuuleri rühmapoliitika keelamine

Selle toimingu peaks soovitavalt tegema saidi IT-administraator.

Toimimisviis

1. Logige instrumenti sisse.
2. Rühmapoliitika redaktori käivitamiseks tippige tegumiriba otsinguväljale `gpedit.msc`.
3. Liikuge jaotisse **Kohaliku arvuti poliitika > Arvuti konfiguratsioon > Haldusmallid > Printerid**.
4. Valige **Luba prindispuuleril** kliendiühendusi aktsepteerida.
5. Topeltklõpsake poliitikal, et seda avada.
6. Valige **Keelatud**.
7. Poliitika salvestamiseks klõpsake nuppu **OK**.
8. Taaskäivitage instrument.

Tulemus

✓ Ülaltoodud etappide läbimine blokeerib sissetulevaid kaugprintimistoiminguid takistades kaugrünnaku vektori. Süsteem ei tööta enam prindiserverina, kuid kohalik printimine otse ühendatud seadmesse on endiselt võimalik.

[9] Microsofti veebisait: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

✓ See rühmapoliitika muudatus määrab järgmise registrivõtme `HKEY_LOCAL_MACHINE\ Software\Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Osuta ja prindi inaktiveerimine Windowsi registris

Soovitame selle toimingu teha IT-administraatoril.

Toimimisviis

1. Logige instrumenti sisse.
2. Tippige tegumiriba otsinguväljale `regedit`, seejärel valige registriredaktor.
3. Liikuge jaotisse `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Kui see on olemas, laiendage printerite haru ja veenduge, et Osuta ja prindi rühma poleks olemas.
   TÄHELEPANU! Printerite haru pole tehasekonfiguratsioonis olemas.
   ⇨ Kui **Osuta ja prindi** rühm on olemas, kontrollige järgmisi sätteid, kui see on olemas, seejärel seadke väärtuseks 0.
   `NoWarningNoElevationOnInstall = 0 või seda pole olemas`
   `UpdatePromptSettings = 0 või seda pole olemas`
5. Taaskäivitage instrument.

Microsoft Windows -taustatulostuksen tietoturva-aukko CVE-2021-34527

("PrintNightmare") Kyberturvallisuuspäivitys Windows 7 -käyttöjärjestelmälle

1 Tietoja päivityksestä

PrintNightmare on Microsoft Windows -käyttöjärjestelmiin (OS) vaikuttava tietoturva-aukko.

Koodin etäsuoritusta koskeva tietoturva-aukko on olemassa, kun Windowsin taustatulostuspalvelu suorittaa virheellisesti etuoikeutetut tiedostotoiminnot. Hyökkääjä, joka onnistuu tämän tietoturva-aukon hyödyntämisessä, voi suorittaa haittaohjelman JÄRJESTELMÄN käyttöoikeuksilla. Tällöin hyökkääjä voi asentaa ohjelmia, tarkastella, muuttaa tai poistaa tietoja tai luoda uusia tilejä, joilla on täydet käyttöoikeudet.[10]

PrintNightmare ei vaikuta ZEISS-laitteiden turvallisuuteen ja suorituskykyyn.

ZEISS suosittelee kuitenkin laitteiden päivittämistä Microsoftin korjaustiedosto- ja/tai rekisteriasetuksilla kyberturvallisuuden jatkumisen varmistamiseksi. ZEISS on analysoinut tietoturva-aukon vaikutuksen ZEISS-tuotteisiin, joissa on Windows-käyttöjärjestelmä, ja vain alla lueteltuihin laitteisiin tarvitaan päivitys.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Poista tulostimen taustatulostuksen ryhmäkäytäntö

On suositeltavaa, että sivuston IT-järjestelmänvalvoja suorittaa tämän tehtävän.

Toimenpide

1. Kirjaudu sisään laitteeseen.
2. Suorita ryhmäkäytäntöeditori kirjoittamalla tehtäväpalkin hakuruutuun `gpedit.msc`.
3. Siirry kohtaan **Paikallisen tietokoneen käytäntö > Tietokoneasetukset > Hallintamallit > Tulostimet**.
4. Hyväksy asiakasyhteydet valitsemalla **Salli taustatulostus**.
5. Avaa käytäntö kaksoisnapsauttamalla sitä.
6. Valitse **Poissa käytöstä**.
7. Tallenna käytäntö valitsemalla **OK**.
8. Käynnistä laite uudelleen.

[10] Microsoft-verkkosivusto: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Tulos

✓ Edellä mainitut toimet estävät etähyökkäysvektorin estämällä saapuvat etätulostustoimet. Järjestelmä ei enää toimi tulostuspalvelimena, mutta paikallinen tulostus suoraan liitettyyn laitteeseen on silti mahdollista.

✓ Tämä ryhmäkäytännön muutos määrittää seuraavan rekisteriavaimen `HKEY_LOCAL_MACHINE\ Software\Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Poista osoittamalla tulostaminen Windowsin rekisterissä

Suosittelemme IT-järjestelmänvalvojaa suorittamaan tämän tehtävän.

Toimenpide

1. Kirjaudu sisään laitteeseen.
2. Kirjoita tehtäväpalkin hakuruutuun `regedit` ja valitse sitten Rekisterieditori.
3. Siirry kohtaan `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Jos Tulostimet-haara on olemassa, laajenna se ja varmista, ettei PointandPrint-ryhmää ole olemassa.
   HUOMIO! Tehdasmääritykset eivät sisällä Tulostimet-haaraa.
   ⇨ Jos **PointandPrint**-ryhmä on olemassa, tarkista seuraavat asetukset, ja jos se on olemassa, aseta arvoksi 0.
   `NoWarningNoElevationOnInstall = 0 tai ei ole olemassa`
   `UpdatePromptSettings = 0 tai ei ole olemassa`
5. Käynnistä laite uudelleen.

Vulnérabilité du spouleur d'impression Microsoft Windows CVE-2021-34527

("PrintNightmare") Mise à jour de cybersécurité pour le système d'exploitation Windows 7

fr ■ 24/09/2021

1 À propos de la mise à jour

PrintNightmare est une vulnérabilité affectant les systèmes d'exploitation (OS) Microsoft Windows.

Il existe une vulnérabilité d'exécution de code à distance lorsque le service Spouleur d'impression Windows exécute de manière incorrecte des opérations sur les fichiers privilégiés. Un attaquant qui parviendrait à exploiter cette vulnérabilité pourrait exécuter du code arbitraire avec les privilèges SYSTEM. Un attaquant pourrait alors installer des programmes, consulter, modifier ou supprimer des données ou créer de nouveaux comptes avec des droits d'utilisateur complets.[11]

PrintNightmare n'affecte pas la sécurité et les performances des appareils ZEISS.

Cependant, ZEISS recommande de mettre à jour les appareils avec le correctif Microsoft et/ou les paramètres du registre, selon le cas, pour assurer une cybersécurité continue. ZEISS a analysé l'impact de cette vulnérabilité sur les produits ZEISS fonctionnant sous Windows OS et seuls les appareils listés ci-dessous doivent exécuter la mise à jour.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Désactiver la politique de groupe du spouleur d'imprimante

Il est recommandé qu'un administrateur informatique du site effectue cette tâche.

Procédure

1. Connectez-vous à l'instrument.
2. Dans la zone de recherche de la barre des tâches, tapez `gpedit.msc` pour exécuter l'éditeur de stratégie de groupe.
3. Accédez à **Stratégie de l'ordinateur local > Configuration de l'ordinateur > Modèles d'administration > Imprimantes**.
4. Sélectionnez **Autoriser le spouleur d'impression** à accepter les connexions des clients.
5. Double-cliquez sur la stratégie pour l'ouvrir.
6. Sélectionnez **Désactivé**.

[11] Site Web de Microsoft : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

7. Sélectionnez **OK** pour enregistrer la stratégie.
8. Redémarrez l'instrument.

Résultat

✓ Les étapes ci-dessus bloqueront le vecteur d'attaque à distance en empêchant les opérations d'impression à distance entrantes. Le système ne fonctionnera plus comme un serveur d'impression, mais l'impression locale sur un périphérique directement connecté sera toujours possible.

✓ Cette modification de la stratégie de groupe va définir la clé de registre suivante `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Désactiver Pointer et imprimer dans le registre Windows

Nous recommandons à un administrateur informatique d'effectuer cette tâche.

Procédure

1. Connectez-vous à l'instrument.
2. Dans la zone de recherche de la barre des tâches, tapez `regedit`, puis sélectionnez Éditeur du registre.
3. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. S'il existe, développez la branche Imprimantes et vérifiez que le groupe PointandPrint n'existe pas.
   AVIS ! La branche Imprimantes n'existe pas dans la configuration d'usine.
   ⇨ Si le groupe **PointandPrint**existe, vérifiez les paramètres suivants, s'il existe, définissez la valeur sur 0.
   `NoWarningNoElevationOnInstall = 0 ou n'existe pas`
   `UpdatePromptSettings = 0 ou n'existe pas`
5. Redémarrez l'instrument.

Sicherheitsrisiko des Microsoft Windows Print Spooler CVE-2021-34527

(„PrintNightmare“) Cybersicherheitsupdate für Windows 7 OS

de ■ 24.09.2021

1 Über das Update

PrintNightmare ist eine Sicherheitslücke, die Microsoft Windows-Betriebssysteme (OS) betrifft.

Es besteht eine Sicherheitslücke bezüglich Remotecodeausführung, wenn der Windows Print Spooler-Dienst unzulässigerweise autorisierte Dateioperationen ausführt. Ein Angreifer, der diese Sicherheitslücke erfolgreich ausnutzt, könnte beliebigen Code mit SYSTEM-Rechten ausführen. Ein Angreifer könnte dann Programme installieren, Daten anzeigen, ändern oder löschen oder neue Konten mit vollen Benutzerrechten erstellen.[12]

PrintNightmare hat keine Auswirkungen auf die Sicherheit und Leistung von ZEISS Geräten.

ZEISS empfiehlt jedoch, die Geräte mit dem Microsoft-Patch und/oder den Registry-Einstellungen zu aktualisieren, um fortgesetzte Cybersicherheit zu gewährleisten. ZEISS hat die Auswirkungen der Sicherheitslücke auf ZEISS Produkte mit dem Windows-Betriebssystem analysiert und nur die unten aufgeführten Geräte müssen das Update ausführen.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Deaktivieren der Druckerspooler-Gruppenrichtlinie

Es wird empfohlen, dass diese Aufgabe von einem Site-IT-Administrator ausgeführt wird.

Vorgehensweise

1. Melden Sie sich bei dem Instrument an.
2. Geben Sie im Suchfeld auf der Taskleiste `gpedit.msc` ein, um den Gruppenrichtlinien-Editor auszuführen.
3. Navigieren Sie zu **Lokale Computerrichtlinie > Computerkonfiguration > Administrative Vorlagen > Drucker**.
4. Wählen **Druckspooler zulassen**, um Clientverbindungen zu akzeptieren.
5. Doppelklicken Sie auf die Richtlinie, um sie zu öffnen.
6. Wählen Sie **Deaktiviert**.
7. Wählen Sie **OK**, um die Richtlinie zu speichern.
8. Starten Sie das Gerät neu.

[12] Microsoft-Website: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Resultat

✓ Wenn Sie die oben genannten Schritte ausführen, wird der Remoteangriffsvektor blockiert, indem eingehende Remotedruckvorgänge verhindert werden. Das System funktioniert nun zwar nicht mehr als Druckserver, das lokale Drucken auf einem direkt angeschlossenen Gerät ist aber weiterhin möglich.

✓ Diese Gruppenrichtlinienänderung stellt den Registrierungsschlüssel auf `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\RegisterSpoolerRemoteRpcEndPoint = 2` ein.

3 Deaktivieren von Point and Print in der Windows-Registrierung

Wir empfehlen, dass ein IT-Administrator diese Aufgabe ausführt.

Vorgehensweise

1. Melden Sie sich bei dem Instrument an.
2. Geben Sie im Suchfeld auf der Taskleiste `regedit` ein, und wählen Sie dann den Registrierungs-Editor aus.
3. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Falls vorhanden, erweitern Sie den Zweig „Drucker“, und stellen Sie sicher, dass die Gruppe „PointandPrint“ nicht vorhanden ist. **HINWEIS! Der Zweig „Drucker“ ist in der Werkskonfiguration nicht vorhanden.**

   ⇨ Wenn die Gruppe **PointandPrint** vorhanden ist, überprüfen Sie die folgenden Einstellungen, und legen Sie, sofern vorhanden, als Wert „0“ fest.
   `NoWarningNoElevationOnInstall = 0 oder nicht vorhanden`
   `UpdatePromptSettings = 0 oder nicht vorhanden`
5. Starten Sie das Gerät neu.

Αδυναμία λογισμικού ουράς εκτύπωσης Microsoft Windows CVE-2021-34527

("PrintNightmare") Ενημέρωση κυβερνοασφάλειας για λειτουργικό σύστημα Windows 7

1 Σχετικά με την ενημέρωση

Το PrintNightmare είναι μια αδυναμία που επηρεάζει τα λειτουργικά συστήματα των Microsoft Windows (OS).

Μια αδυναμία απομακρυσμένης εκτέλεσης κώδικα υπάρχει όταν η υπηρεσία του λογισμικού ουράς εκτύπωσης των Windows εκτελεί εσφαλμένα λειτουργίες προνομιούχων αρχείων. Ένας εισβολέας που εκμεταλλεύτηκε με επιτυχία αυτήν την αδυναμία θα μπορούσε να εκτελέσει οποιονδήποτε κώδικα με προνόμια ΣΥΣΤΗΜΑΤΟΣ. Ένας εισβολέας θα μπορούσε στη συνέχεια να εγκαταστήσει προγράμματα, να προβάλλει, αλλάξει ή διαγράψει δεδομένα ή να δημιουργήσει νέους λογαριασμούς με πλήρη δικαιώματα χρήστη.[13]

Το PrintNightmare δεν επηρεάζει την ασφάλεια και την απόδοση σε καμία από τις συσκευές ZEISS.

Ωστόσο, η ZEISS συνιστά την ενημέρωση συσκευών με την ενημέρωση κώδικα της Microsoft ή/και τις ρυθμίσεις μητρώου, κατά περίπτωση, για να διασφαλίσει τη συνεχή κυβερνοασφάλεια. Η ZEISS ανέλυσε τον αντίκτυπο της αδυναμίας που έχουν τα προϊόντα ZEISS που εκτελούν λειτουργικό σύστημα Windows και μόνο οι συσκευές που αναφέρονται παρακάτω πρέπει να εκτελέσουν την ενημέρωση.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Απενεργοποίηση της Πολιτικής ομάδας λογισμικών ουράς εκτύπωσης

Συνιστάται η εκτέλεση αυτής της εργασίας από Διαχειριστή συστημάτων πληροφορικής του ιστότοπου.

Μεθόδευση

1. Συνδεθείτε στο όργανο.
2. Στο πλαίσιο αναζήτησης στη γραμμή εργασιών, πληκτρολογήστε `gpedit.msc` για να εκτελέσετε το πρόγραμμα επεξεργασίας Πολιτικής ομάδας.
3. Μεταβείτε στην **Πολιτική τοπικού υπολογιστή > Διαμόρφωση υπολογιστή > Διαχειριστικά πρότυπα > Εκτυπωτές**.
4. Επιλέξτε **Να επιτρέπεται το Λογισμικό ουράς εκτύπωσης** να αποδέχεται συνδέσεις πελάτη.
5. Κάντε διπλό κλικ στην πολιτική για να την ανοίξετε.

[13] Ιστότοπος της Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

6. Επιλέξτε **Απενεργοποιημένη**.
7. Επιλέξτε **OK** για να αποθηκεύσετε την πολιτική.
8. Επανεκκινήστε το όργανο.

Αποτέλεσμα

✓ Η εκτέλεση των παραπάνω βημάτων θα αποκλείσει την απομακρυσμένη επίθεση αποτρέποντας τις εισερχόμενες λειτουργίες απομακρυσμένης εκτύπωσης. Το σύστημα δεν θα λειτουργεί πλέον ως διακομιστής εκτύπωσης, αλλά η τοπική εκτύπωση σε μια άμεσα συνδεδεμένη συσκευή θα εξακολουθεί να είναι δυνατή.

✓ Αυτή η αλλαγή Πολιτικής ομάδας θα ορίσει το ακόλουθο κλειδί μητρώου `HKEY_LOCAL_MACHINE\ Λογισμικό \Πολιτικές\Microsoft\Windows NT\Εκτυπωτές \ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Απενεργοποιήστε το Point and Print στο Μητρώο των Windows

Συνιστούμε την εκτέλεση αυτής της εργασίας από έναν διαχειριστή συστημάτων πληροφορικής.

Μεθόδευση

1. Συνδεθείτε στο όργανο.
2. Στο πλαίσιο αναζήτησης στη γραμμή εργασιών, πληκτρολογήστε `regedit`και, στη συνέχεια, επιλέξτε "Πρόγραμμα επεξεργασίας μητρώου".
3. Μεταβείτε στο `HKEY_LOCAL_MACHINE\SOFTWARE \Policies\Microsoft\Windows NT\Printers`.
4. Εάν υπάρχει, αναπτύξτε το τμήμα "Εκτυπωτές" και βεβαιωθείτε ότι η ομάδα PointandPrint δεν υπάρχει.
   ΥΠΟΔΕΙΞΗ! Το τμήμα "Εκτυπωτές" δεν υπάρχει στην εργοστασιακή διαμόρφωση.
   ⇨ Εάν υπάρχει η ομάδα **PointandPrint**, ελέγξτε τις ακόλουθες ρυθμίσεις και εφόσον υπάρχει, ορίστε την τιμή σε 0 .
   `NoWarningNoElevationOnInstall = 0 ή δεν υπάρχει`
   `UpdatePromptSettings = 0 ή δεν υπάρχει`
5. Επανεκκινήστε το όργανο.

Microsoft Windows Nyomtatásisor-kezelő biztonsági rése CVE-2021-34527

(„PrintNightmare”) Kiberbiztonsági frissítés Windows 7 operációs rendszerhez

hu ■ 2021. 09. 24.

Microsoft Windows Nyomtatásisor-kezelő biztonsági rése CVE-2021-34527

1 A frissítésről

A PrintNightmare a Microsoft Windows operációs rendszereket (OS) érintő biztonsági rés.

Távoli kódfuttatási biztonsági rés áll fenn, ha a Windows Nyomtatásisor-kezelő szolgáltatás helytelenül hajt végre privilegizált fájlműveleteket. A biztonsági rést sikeresen kihasználó támadó tetszőleges kódot tud futtatni SYSTEM jogosultságokkal. A támadó ezután programokat telepíthet; adatokat tud megtekinteni, módosítani vagy törölni; illetve új fiókokat hozhat létre teljes körű felhasználói jogokkal.[14]

A PrintNightmare nincs hatással a ZEISS-eszközök biztonságára és teljesítményére.

A ZEISS azonban azt javasolja, hogy a folyamatos kiberbiztonság biztosítása érdekében frissítse az eszközöket a Microsoft javításával és/vagy a beállításjegyzék-beállításokkal. A ZEISS elemezte a biztonsági rés hatását a Windows operációs rendszert futtató ZEISS termékekre, és csak az alább felsorolt eszközöknek kell futtatniuk a frissítést.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 A Nyomtatásisor-kezelő csoportházirend letiltása

Javasoljuk, hogy a webhely informatikai rendszergazdája végezze el ezt a műveletet.

Eljárásmód

1. Jelentkezzen be az eszközön.
2. A Csoportházirend-szerkesztő futtatásához a tálca keresőmezőjében írja be a következőt: `gpedit.msc`.
3. Nyissa meg a következőt: **Házirend: Helyi számítógép > Számítógép konfigurációja > Felügyeleti Sablonok > Nyomtatók**.
4. Válassza a **Ügyfélkapcsolatok elfogadásának engedélyezése a Nyomtatásisor-kezelő számára** lehetőséget.
5. Kattintson duplán a házirend megnyitásához.
6. Válassza a **Letiltva** lehetőséget.
7. A házirend mentéséhez kattintson az **OK** gombra.
8. Indítsa újra az eszközt.

[14] A Microsoft webhelye: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Eredmény

✓ A fenti lépések elvégzése blokkolja a távoli támadásvektort azáltal, hogy megakadályozza a beérkező távoli nyomtatási műveletek végrehajtását. A rendszer ezután nem fog nyomtatókiszolgálóként működni, de a helyi nyomtatás továbbra is lehetséges egy közvetlenül csatlakoztatott eszközzel.

✓ Ez a csoportházirend-módosítás a következő rendszerleíró kulcsot állítja be: `HKEY_LOCAL_MACHINE\ Software \Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 A Windows beállításjegyzékében inaktiválja a Gyorsnyomtatást

Javasoljuk, hogy informatikai rendszergazda végezze el ezt a műveletet.

Eljárásmód

1. Jelentkezzen be az eszközön.
2. A tálca keresőmezőjében írja be a következőt: `regedit`, majd válassza a Beállításszerkesztő lehetőséget.
3. Nyissa meg a következőt: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Ha létezik, bővítse ki a Nyomtatók ágat, és győződjön meg arról, hogy a PointandPrint csoport nem létezik.
   UTALÁS! A Nyomtatók ág nem létezik a gyári konfigurációban.
   ⇨ Ha a **PointandPrint** csoport létezik, ellenőrizze a következő beállításokat, ha létezik, akkor állítsa az értéket 0-ra.
   `NoWarningNoElevationOnInstall = 0 vagy nem létezik`
   `UpdatePromptSettings = 0 vagy nem létezik`
5. Indítsa újra az eszközt.

Vulnerabilità dello spooler di stampa di Microsoft Windows CVE-2021-34527

("PrintNightmare") Aggiornamento della sicurezza informatica per il sistema operativo Windows 7

it ■ 24/09/2021

1 Informazioni sull'aggiornamento

PrintNightmare è una vulnerabilità che interessa i sistemi operativi Microsoft Windows.

Esiste una vulnerabilità legata all'esecuzione del codice in modalità remota quando il servizio Spooler di stampa di Windows esegue in modo erroneo operazioni sui file privilegiati. Sfruttando questa vulnerabilità, un utente malintenzionato può eseguire un codice arbitrario con privilegi SYSTEM. Un utente malintenzionato potrebbe quindi installare programmi, visualizzare, modificare o eliminare i dati, oppure creare nuovi account con diritti utente completi.[15]

PrintNightmare non influisce sulla sicurezza e sulle prestazioni di nessuno dei dispositivi ZEISS.

Tuttavia, ZEISS consiglia di aggiornare i dispositivi con la patch Microsoft e/o le impostazioni del Registro di sistema, in base ai casi, per garantire la sicurezza informatica continua. ZEISS ha analizzato l'impatto della vulnerabilità sui prodotti ZEISS che eseguono il sistema operativo Windows e solo i dispositivi elencati di seguito devono eseguire l'aggiornamento.

- CIRRUS 400/4000
- CIRRUS 500/5000
- Foto CIRRUS 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Disabilitare Criteri di gruppo dello spooler di stampa

Si consiglia che questa attività venga eseguita da un amministratore IT del sito.

Procedura

1. Accedere allo strumento.
2. Nella casella di ricerca, sulla barra delle applicazioni, digitare `gpedit.msc` per eseguire l'editor Criteri di gruppo.
3. Andare a **Criteri del computer locale > Configurazione computer > Modelli amministrativi > Stampanti**.
4. Selezionare **Consenti a Spooler di stampa** di accettare connessioni client.
5. Fare doppio clic sul criterio per aprirlo.
6. Selezionare **Disattivato**.
7. Selezionare **OK** per salvare il criterio.
8. Riavviare lo strumento.

[15] Sito Web Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Risultato

- ✓ L'operazione descritta in precedenza bloccherà il vettore di attacco remoto impedendo le operazioni di stampa remota in ingresso. Il sistema non funzionerà più come server di stampa, ma sarà comunque possibile stampare localmente su un dispositivo collegato direttamente.
- ✓ Questa modifica di Criteri di gruppo consente di impostare la seguente chiave del Registro di sistema:
  `HKEY_LOCAL_MACHINE\ Software\Policies \Microsoft\Windows NT\Printers\ Register-SpoolerRemoteRpcEndPoint = 2`

3 Disattivare Point and Print nel Registro di sistema di Windows

Si consiglia che questa attività venga eseguita da un amministratore IT.

Procedura

1. Accedere allo strumento.
2. Nella casella di ricerca sulla barra delle applicazioni digitare `regedit`, quindi selezionare Editor del Registro di sistema.
3. Andare a `HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows NT\Printers`.
4. Se esiste, espandere il ramo Stampanti e assicurarsi che il gruppo PointandPrint non esista.
   AVVISO! Il ramo Stampanti non esiste nella configurazione di fabbrica.
   - ⇨ Se il gruppo **PointandPrint** esiste, controllare le impostazioni che seguono, quindi impostare il valore su 0.
     `NoWarningNoElevationOnInstall = 0 o non esiste`
     `UpdatePromptSettings = 0 o non esiste`
5. Riavviare lo strumento.

Microsoft Windows の印刷スプーラーの脆弱性 CVE-2021-34527

(「PrintNightmare」) Windows 7 OS 用のサイバーセキュリティ更新プログラム

1 更新プログラムについて

PrintNightmare は、Microsoft Windows オペレーティングシステム (OS) に影響を与える脆弱性です。

Windows 印刷スプーラーサービスにより特権ファイル操作が不適切に実行された場合に、リモートでコードが実行される脆弱性が存在します。攻撃者がこの脆弱性を悪用した場合、SYSTEM 特権を使用して任意のコードを実行する可能性があります。その後、攻撃者はプログラムのインストール、データの表示、変更、削除などを行ったり、あらゆるユーザー権限を持つ新しいアカウントを作成したりする可能性があります。☒[16]

PrintNightmare は、ZEISS デバイスの安全性とパフォーマンスには影響しません。

しかし、サイバーセキュリティを確実に維持するために、Microsoft のパッチやレジストリ設定 (該当する場合) を使用してデバイスを更新することをお勧めします。当社は、Windows OS を実行している ZEISS 製品に対するこの脆弱性の影響を分析しました。アップデートを実行する必要があるのは以下のデバイスのみとなります。

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS フォト 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 印刷スプーラーのグループポリシーを無効にする

このタスクは、サイトの IT 管理者が実行することをお勧めします。

方法

1. 装置にログインします。
2. タスクバーの検索ボックスに「`gpedit.msc`」と入力して、グループポリシーエディターを実行します。
3. **[ローカル コンピューター ポリシー] > [コンピューターの構成] > [管理用テンプレート] > [プリンター]** に移動します。
4. [**印刷スプーラー**にクライアント接続の受け入れを許可する] を選択します。
5. ポリシーをダブルクリックして開きます。
6. [**無効**] を選択します。
7. [**OK**] を選択してポリシーを保存します。
8. 装置を再起動します。

結果

✓ 上記の手順を実行すると、リモート印刷操作の受信を防ぐことでリモート攻撃ベクトルがブロックされます。システムはプリントサーバーとして機能しなくなりますが、直接接続されたデバイスへのローカル印刷は引き続き利用できます。

[16] Microsoft の Web サイト: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

✓ このグループポリシーの変更により、レジストリキー `HKEY_LOCAL_MACHINE\ Software\Policies\Microsoft\Windows NT\Printers\RegisterSpoolerRemoteRpcEndPoint = 2` が設定されます。

3 Windows レジストリでポイントアンドプリントを無効にする

このタスクは IT 管理者が実行することをお勧めします。

方法

1. 装置にログインします。
2. タスクバーの検索ボックスに「`regedit`」と入力し、[レジストリ エディター] を選択します。
3. `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers` に移動します。
4. [Printers] ブランチがある場合は展開し、[PointandPrint] グループが存在しないことを確認します。
   注記! [Printers] ブランチは既定の設定では存在しません。
   ⇨ [**PointandPrint**] グループが存在する場合は、次の設定を確認し、存在する場合は値を「0」に設定します。
   `NoWarningNoElevationOnInstall = 0` または存在しない
   `UpdatePromptSettings = 0` または存在しない
5. 装置を再起動します。

Microsoft Windows 인쇄 스풀러 취약성
CVE-2021-34527
("PrintNightmare") Windows 7 OS에 대한 사이버 보안 업데이트

Microsoft Windows 인쇄 스풀러 취약성 CVE-2021-34527

1 업데이트 정보

PrintNightmare는 Microsoft Windows 운영 체제(OS)에 영향을 미치는 취약성을 말합니다.

Windows 인쇄 스풀러 서비스가 권한 있는 파일 작업을 부적절하게 수행할 때 원격 코드 실행 취약성이 존재합니다. 이 취약성을 악용한 공격자는 SYSTEM 권한으로 임의코드를 실행할 수 있습니다. 그런 다음 공격자는 프로그램을 설치할 수 있습니다. 데이터를 확인, 변경 또는 삭제하거나 전체 사용자 권한이 있는 새 계정을 만듭니다.[17]

PrintNightmare는 ZEISS 장치의 안전성과 성능에 영향을 미치지 않습니다.

그러나 ZEISS는 지속적인 사이버 보안을 보장하기 위해 Microsoft 패치 및/또는 레지스트리 설정으로 장치를 업데이트하는 것이 좋습니다. ZEISS는 Windows OS를 실행하는 ZEISS 제품에 대한 취약성의 영향을 분석했으며 아래에 나열된 장치에만 업데이트를 실행해야 합니다.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS 포토 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 프린터 스풀러 그룹 정책 비활성화

사이트 IT 관리자가 이 작업을 수행하는 것이 좋습니다.

수행 방법

1. 기기에 로그인합니다.
2. 작업 표시줄의 검색 상자에 `gpedit.msc`를 입력하여 그룹 정책 편집기를 실행합니다.
3. **로컬 컴퓨터 정책 > 컴퓨터 구성 > 관리 템플릿 > 프린터**로 이동합니다.
4. **인쇄 스풀러 허용**을 선택하여 클라이언트 연결을 수락합니다.
5. 정책을 더블 클릭하여 엽니다.
6. **사용 안 함** 선택합니다.
7. **확인**을 선택하여 정책을 저장합니다.
8. 기기를 다시 시작합니다.

처리 결과

✓ 위의 단계를 수행하면 인바운드 원격 인쇄 작업을 방지하여 원격 공격 벡터를 차단합니다. 시스템은 더 이상 인쇄 서버로 작동하지 않지만 직접 연결된 장치에 대한 로컬 인쇄는 여전히 가능합니다.

[17] Microsoft 웹사이트: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

✓ 이 그룹 정책 변경은 다음 레지스트리 키 `HKEY_LOCAL_MACHINE\ Software\Policies\Microsoft\Windows NT\Printers\RegisterSpoolerRemoteRpcEndPoint = 2`를 설정합니다

3 Windows 레지스트리에서 포인트 및 인쇄 비활성화

IT 관리자가 이 작업을 수행하는 것이 좋습니다.

수행 방법

1. 기기에 로그인합니다.
2. 작업 표시줄의 검색 상자에 `regedit`을 입력한 다음 레지스트리 편집기를 선택합니다.
3. `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`로 이동합니다.
4. 이 경우 프린터 분기를 확장하고 PointandPrint 그룹이 존재하지 않는지 확인합니다.
   참고! 프린터 분기는 공장 구성에 존재하지 않습니다.
   ⇨ **PointandPrint** 그룹이 있는 경우 다음 설정을 확인하고 설정이 있는 경우 값을 0으로 설정합니다.
   `NoWarningNoElevationOnInstall = 0` 또는 존재하지 않음
   `UpdatePromptSettings = 0` 또는 존재하지 않음
5. 기기를 다시 시작합니다.

Microsoft Windows drukas spolētāja ievainojamība CVE-2021-34527

("PrintNightmare") Kiberdrošības atjauninājums operētājsistēmai Windows 7

1 Par atjauninināšanu

PrintNightmare ir ievainojamība, kas ietekmē Microsoft Windows operētājsistēmas (OS).

Attālā koda izpildes ievainojamība pastāv, ja Windows drukas spolētāja pakalpojums nepareizi veic priviliģētas failu darbības. Uzbrucējs, kurš veiksmīgi izmantoja šo ievainojamību, var palaist patvaļīgu kodu ar SYSTEM privilēģijām. Pēc tam uzbrucējs var instalēt programmas; skatīt, mainīt vai dzēst datus; vai izveidot jaunus kontus ar pilnām lietotāja tiesībām.[18]

PrintNightmare neietekmē drošību un veiktspēju nevienā ZEISS ierīcē.

Tomēr ZEISS iesaka atjaunināt ierīces ar Microsoft ielāpa un/vai reģistra iestatījumiem, lai nodrošinātu nepārtrauktu kiberdrošību. ZEISS ir analizējis ievainojamības ietekmi uz ZEISS produktiem, kuros darbojas Windows operētājsistēma, un atjauninājums ir jāpalaiž tikai tālāk uzskaitītajām ierīcēm.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Atspējot drukas spolētāja grupas politiku

Ieteicams vietnes IT administratoram veiktu šo uzdevumu.

Darbība

1. Piesakieties instrumentā.
2. Uzdevumjoslas meklēšanas lodziņā ierakstiet `gpedit.msc`, lai palaistu grupas politikas redaktoru.
3. Naviģējiet uz **Lokālā datora politika > Datora konfigurācija > Administratīvās veidnes > Printeri**.
4. Atlasiet **Atļaut drukas spolētāju**, lai akceptētu klienta savienojumus.
5. Veiciet dubultklikšķi uz politikas, lai to atvērtu.
6. Atlasiet **Atspējots**.
7. Atlasiet **Labi**, lai saglabātu politiku.
8. Restartējiet instrumentu.

Rezultāts

✓ Veicot iepriekš minētās darbības, tiks bloķēts attālā uzbrukuma vektors, novēršot ienākošās attālās drukāšanas darbības. Sistēma vairs nedarbosies kā drukas serveris, bet joprojām būs iespējama vietējā drukāšana tieši pievienotā ierīcē.

[18] Microsoft tīmekļa vietne: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

✓ Šīs grupas politikas izmaiņas iestatīs šādu reģistra atslēgu `HKEY_LOCAL_MACHINE\ Software\Policies \Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Deaktivizēt punktu un drukāt Windows reģistrā

Iesakām šo uzdevumu veikt IT administratoru.

Darbība

1. Piesakieties instrumentā.
2. Uzdevumjoslas meklēšanas lodziņā ierakstiet `regedit` , pēc tam atlasiet Reģistra redaktors.
3. Naviģējiet uz `HKEY_LOCAL_MACHINE\SOFTWARE \Policies\Microsoft\Windows NT\Printers`.
4. Ja tāds pastāv, izvērsiet zaru Printeri un pārliecinieties, vai grupa PointandPrint nepastāv.
   NORĀDĪJUMS! Rūpnīcas konfigurācijā nav zara Printeri.
   ⇨ Ja grupa **PointandPrint** pastāv, pārbaudiet šādus iestatījumus, ja tādi ir, pēc tam iestatiet vērtību uz 0 .
   `NoWarningNoElevationOnInstall = 0 or does not exist`
   `UpdatePromptSettings = 0 or does not exist`
5. Restartējiet instrumentu.

„Microsoft Windows“ spausdinimo kaupos pažeidžiamumas CVE-2021-34527

(„PrintNightmare“) kibernetinio saugumo naujinys „Windows 7“ OS

„Microsoft Windows“ spausdinimo kaupos pažeidžiamumas CVE-2021-34527

1 Apie naujinį

„PrintNightmare“ yra pažeidžiamumas, turintis įtakos „Microsoft Windows“ operacinėms sistemoms (OS).

Nuotolinio kodo vykdymo pažeidžiamumas yra, kai „Windows“ spausdinimo kaupos tarnyba netinkamai atlieka privilegijuotų failų operacijas. Pažeidėjas, sėkmingai išnaudojęs šį pažeidžiamumą, gali paleisti savavališką kodą su SISTEMOS teisėmis. Tada pažeidėjas gali įdiegti programas; peržiūrėti, keisti arba naikinti duomenis, arba sukurti naujas paskyras su visomis naudotojo teisėmis.[19]

„PrintNightmare“ neturi įtakos jokių ZEISS įrenginių saugai ir veikimui.

Tačiau ZEISS rekomenduoja atnaujinti įrenginius naudojant „Microsoft“ pataisą ir (arba) registro parametrus, kaip tinkama, kad būtų užtikrintas nuolatinis kibernetinis saugumas. ZEISS išanalizavo pažeidžiamumo poveikį ZEISS gaminiams, kuriuose veikia „Windows“ OS, ir tik toliau išvardytiems įrenginiams turi būti paleistas naujinys.

- CIRRUS 400/4000
- CIRRUS 500/5000
- „CIRRUS Photo“ 600 / 800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Pasyvinkite spausdintuvo kaupos grupės politiką

Rekomenduojama, kad šią užduotį atliktų įmonės IT administratorius.

Veiksmai

1. Prisijunkite prie instrumento.
2. Užduočių juostos ieškos lauke įrašykite `gpedit.msc`, kad paleistumėte grupės politikos rengyklę.
3. Eikite į **Local Computer Policy > Computer Configuration > Administrative Templates > Printers**.
4. Pasirinkite **Allow Print Spooler**, kad priimtų kliento jungtis.
5. Dukart spustelėkite politiką, kad ją atidarytumėte.
6. Pasirinkite **Disabled**.
7. Pasirinkite **OK**, kad įrašytumėte politiką.
8. Paleiskite instrumentą iš naujo.

[19] „Microsoft“ žiniatinklio svetainė: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Rezultatas

- ✓ Atlikus pirmiau nurodytus veiksmus bus blokuojamas nuotolinės atakos vektorius, užkertant kelią įeinančioms nuotolinio spausdinimo operacijoms. Sistema nebeveiks kaip spausdinimo serveris, tačiau vietos spausdinimas tiesiogiai prijungtame įrenginyje vis tiek bus galimas.
- ✓ Šis grupės strategijos pakeitimas nustatys šį registro raktą `HKEY_LOCAL_MACHINE\ Software\Policies \Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Pasyvinkite tašką ir spausdinimą „Windows“ registre

Šią užduotį atlikti rekomenduojame IT administratoriui.

Veiksmai

1. Prisijunkite prie instrumento.
2. Užduočių juostos ieškos lauke įrašykite `regedit`, tada pasirinkite „Registry Editor“.
3. Eikite į `HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows NT\Printers`.
4. Jei yra, išplėskite šaką „Printers“ ir įsitikinkite, kad grupės „PointandPrint“ nėra.
   NURODYMAS! Šakos „Printers“ gamyklos konfigūracijoje nėra.
   - ⇨ Jei grupė **PointandPrint** yra, patikrinkite tolesnius parametrus, jei yra, nustatykite reikšmę 0.
     `NoWarningNoElevationOnInstall = 0 arba nėra`
     `UpdatePromptSettings = 0 arba nėra`
5. Paleiskite instrumentą iš naujo.

Sikkerhetsproblem i utskriftskøen i Microsoft Windows CVE-2021-34527

("PrintNightmare") Cybersikkerhetsoppdatering for Windows 7 OS

1 Om oppdateringen

PrintNightmare er et sikkerhetsproblem som berører Microsoft Windows-operativsystemer (OS).

Det finnes et sikkerhetsproblem som kan forårsake ekstern kjøring av kode når utskriftskøtjenesten i Windows utfører privilegerte fil-operasjoner på feil måte. En angriper som klarer å utnytte dette sikkerhetsproblemet, kan kjøre vilkårlig kode med SYSTEM-rettigheter. En angriper kan deretter installere programmer, vise, endre eller slette data, eller opprette nye kontoer med fullstendige brukerrettigheter.[20]

PrintNightmare påvirker ikke sikkerheten og ytelsen på noen av ZEISS-enhetene.

ZEISS anbefaler imidlertid å oppdatere enheter med Microsoft-oppdateringen og/eller registerinnstillingene, der det er aktuelt, for å sikre fortsatt cybersikkerhet. ZEISS har analysert virkningen av sikkerhetsproblemet på ZEISS-produkter som kjører Windows OS, og bare enheter som er oppført nedenfor, må kjøre oppdateringen.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Deaktiver gruppepolicyen for utskriftskøen

Det anbefales at en IT-administrator for området utfører denne oppgaven.

Fremgangsmåte

1. Logge på instrumentet.
2. I søkeboksen på oppgavelinjen skriver du inn `gpedit.msc` for å kjøre redigeringsprogrammet for gruppepolicy.
3. Gå til **Lokal datamaskinpolicy > Datamaskinkonfigurasjon > Administrative maler > Skrivere**.
4. Velg **Lar utskriftskøen** godta klienttilkoblinger.
5. Dobbeltklikk på policyen for å åpne den.
6. Velg **Deaktivert**.
7. Velg **OK** for å lagre policyen.
8. Start instrumentet på nytt.

[20] Microsofts nettsted: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Resultat

✓ Hvis du utfører trinnene ovenfor, blokkeres den eksterne angrepsvektoren ved å forhindre innkommende eksterne utskriftsoperasjoner. Systemet vil ikke lenger fungere som en utskriftsserver, men lokal utskrift til en direkte tilkoblet enhet vil fortsatt være mulig.

✓ Denne gruppepolicyendringen angir følgende registernøkkel `HKEY_LOCAL_MACHINE\ Software\Policies \Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Deaktiver pek og skriv ut i Windows-registeret

Vi anbefaler at en IT-administrator utfører denne oppgaven.

Fremgangsmåte

1. Logge på instrumentet.
2. Skriv inn `regedit` i søkeboksen på oppgavelinjen, og velg deretter Registerredigering.
3. Gå til `HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows NT\Printers`.
4. Hvis den finnes, utvider du grenen Skrivere og kontrollerer at PointandPrint-gruppen ikke finnes.
   MERKNAD! Grenen Skrivere finnes ikke i fabrikkkonfigurasjonen.
   ⇨ Hvis **PointandPrint**-gruppen finnes, kontrollerer du følgende innstillinger, og deretter setter du verdien til 0.
   `NoWarningNoElevationOnInstall = 0 eller finnes ikke`
   `UpdatePromptSettings = 0 eller finnes ikke`
5. Start instrumentet på nytt.

Luka w zabezpieczeniach bufora wydruku systemu Microsoft Windows CVE-2021-34527

(„PrintNightmare”) Aktualizacja funkcji cyberbezpieczeństwa dla systemu operacyjnego Windows 7

pl ■ 24.09.2021

Luka w zabezpieczeniach bufora wydruku systemu Microsoft Windows CVE-2021-34527

1 O aktualizacji

PrintNightmare to luka w zabezpieczeniach systemów operacyjnych (OS) Microsoft Windows.

Luka w zabezpieczeniach umożliwiająca zdalne wykonanie kodu powstaje, gdy usługa Bufor wydruku systemu Windows nieprawidłowo wykonuje uprzywilejowane operacje na plikach. Napastnik, który z powodzeniem wykorzysta tę lukę, może uruchomić dowolny kod z uprawnieniami SYSTEM. Napastnik może wówczas instalować programy; przeglądać, zmieniać lub usuwać dane; może też tworzyć nowe konta z pełnymi prawami użytkownika.[21]

PrintNightmare nie wpływa na bezpieczeństwo i wydajność żadnego z urządzeń ZEISS.

Firma ZEISS zaleca jednak aktualizację urządzeń za pomocą poprawki firmy Microsoft lub ustawień rejestru, zależnie od sytuacji, w celu zapewnienia ciągłości cyberbezpieczeństwa. Firma ZEISS przeanalizowała wpływ tej luki w produktach ZEISS z systemem operacyjnym Windows i uruchomienie aktualizacji jest konieczne wyłącznie w przypadku poniższych urządzeń.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Wyłącz zasady grupy bufora drukarki

Zaleca się, aby zadanie to wykonał administrator IT witryny.

Sposób postępowania

1. Zaloguj się do urządzenia.
2. W polu wyszukiwania na pasku zadań wpisz `gpedit.msc`, aby uruchomić edytor zasad grupy.
3. Przejdź do **Zasady komputera lokalnego > Konfiguracja komputera > Szablony administracyjne > Drukarki**.
4. Wybierz **Zezwalaj na bufor wydruku**, aby zaakceptować połączenia klienta.
5. Kliknij dwukrotnie zasady, aby je otworzyć.
6. Wybierz **Wyłączone**.
7. Wybierz **OK**, aby zapisać zasady.
8. Uruchom ponownie urządzenie.

[21] Witryna internetowa firmy Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Wynik

✓ Wykonanie powyższych czynności zablokuje wektor zdalnego ataku poprzez uniemożliwienie operacji zdalnego drukowania przychodzącego. System nie będzie już działał jako serwer druku, ale nadal będzie możliwe drukowanie lokalne na bezpośrednio podłączonym urządzeniu.

✓ Ta zmiana zasad grupy spowoduje ustawienie następującego klucza rejestru `HKEY_LOCAL_MACHINE\ Software \Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Wyłącz funkcję „Wskaż i drukuj” w rejestrze systemu Windows

Zaleca się, aby wykonał to zdalnie administrator IT witryny.

Sposób postępowania

1. Zaloguj się do urządzenia.
2. W polu wyszukiwania na pasku zadań wpisz `regedit`, a następnie wybierz Edytor rejestru.
3. Przejdź do `HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows NT\Printers`.
4. Jeśli gałąź Drukarki istnieje, rozwiń ją i sprawdź, czy grupa PointandPrint nie istnieje.
   WSKAZÓWKA! W konfiguracji fabrycznej gałąź Drukarki nie istnieje.
   ⇨ Jeśli grupa **PointandPrint** istnieje, sprawdź następujące ustawienia; jeśli istnieje, ustaw wartość na 0.
   `NoWarningNoElevationOnInstall = 0 lub nie istnieje`
   `UpdatePromptSettings= 0 lub nie istnieje`
5. Uruchom ponownie urządzenie.

Vulnerabilidade no Spooler de Impressão do Microsoft Windows CVE-2021-34527

Atualização de cibersegurança para o sistema operativo Windows 7 ("PrintNightmare")

pt ■ 24/09/2021

Vulnerabilidade no Spooler de Impressão do Microsoft Windows
CVE-2021-34527

1 Sobre a atualização

O PrintNightmare é uma vulnerabilidade que afeta os sistemas operativos (SO) Microsoft Windows.

Existe uma vulnerabilidade de execução remota de código quando o serviço Spooler de Impressão do Windows executa incorretamente operações de ficheiro com privilégios. Um atacante que conseguir explorar esta vulnerabilidade poderá executar código arbitrário com privilégios do SISTEMA. O atacante poderá assim instalar programas; ver, alterar ou eliminar dados ou criar novas contas com direitos plenos de utilizador.[22]

O PrintNightmare não afeta a segurança nem o desempenho em nenhum dos dispositivos ZEISS.

No entanto, a ZEISS recomenda atualizar os dispositivos com as definições de patch e/ou registo da Microsoft, conforme aplicável, para garantir a continuidade da cibersegurança. A ZEISS analisou o impacto da vulnerabilidade nos produtos ZEISS que executam o sistema operativo Windows. Apenas os dispositivos indicados abaixo têm de executar a atualização.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Desative a Política de Grupo de Spooler de Impressão

Recomenda-se que esta tarefa seja realizada por um administrador de TI do local.

Procedimento

1. Inicie sessão no instrumento.
2. Na caixa de pesquisa da barra de tarefas, escreva `gpedit.msc` para executar o editor de Política de Grupo.
3. Navegue para **Política do Computador Local > Configuração do Computador > Modelos Administrativos > Impressoras**.
4. Selecione **Permitir Spooler de Impressão** para aceitar ligações de clientes.
5. Clique duas vezes na política para a abrir.
6. Selecione **Desativada**.
7. Selecione **OK** para guardar a política.
8. Reinicie o instrumento.

[22] Site da Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Resultado

✓ Executar os passos acima irá bloquear o vetor de ataque remoto, impedindo a entrada de operações remotas de impressão. O sistema deixará de funcionar como um servidor de impressão, mas a impressão local num dispositivo ligado diretamente continuará a ser possível.

✓ Esta alteração na Política de Grupo irá definir a seguinte chave de registo `HKEY_LOCAL_MACHINE\ Software \Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Desative a opção Apontar e Imprimir no Registo do Windows

Recomendamos que esta tarefa seja realizada por um administrador de TI.

Procedimento

1. Inicie sessão no instrumento.
2. Na caixa de pesquisa da barra de tarefas, escreva `regedit` e, em seguida, selecione Editor de registo.
3. Navegue para `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Se existir, expanda o ramo Impressoras e certifique-se de que o grupo PointandPrint (Apontar e Imprimir) não existe.
   NOTA! O ramo Impressoras não existe na configuração de fábrica.
   ⇨ Se o grupo **PointandPrint** (Apontar e imprimir) existir, verifique as seguintes definições. Se existir, então defina o valor como 0.
   `NoWarningNoElevationOnInstall = 0 ou não existe`
   `UpdatePromptSettings = 0 ou não existe`
5. Reinicie o instrumento.

Vulnerabilidade no spooler de impressão do Microsoft Windows CVE-2021-34527

Atualização de segurança cibernética para o sistema operacional Windows 7 ("PrintNightmare")

pt-br ■ 24/09/2021

Vulnerabilidade no spooler de impressão do Microsoft Windows CVE-2021-34527

1 Sobre a atualização

O PrintNightmare é uma vulnerabilidade que afeta os sistemas operacionais (SO) Microsoft Windows.

Existe uma vulnerabilidade de execução remota de código quando o serviço de spooler de impressão do Windows executa indevidamente operações de arquivo privilegiadas. Um invasor que conseguiu explorar com sucesso essa vulnerabilidade pode executar código arbitrário com privilégios de SISTEMA. Um invasor poderia então instalar programas; exibir, alterar ou excluir dados ou criar novas contas com direitos plenos de usuário.[23]

O PrintNightmare não afeta a segurança nem o desempenho em nenhum dos dispositivos ZEISS.

No entanto, a ZEISS recomenda atualizar os dispositivos com as configurações de patch e/ou registro da Microsoft, conforme aplicável, para garantir continuidade da segurança cibernética. A ZEISS analisou o impacto da vulnerabilidade nos produtos ZEISS que executam o sistema operacional Windows. Apenas os dispositivos listados abaixo devem executar a atualização.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Desative a política de grupo de spooler de impressão

Recomenda-se que essa tarefa seja realizada por um administrador de TI do local.

Procedimento

1. Faça login no instrumento.
2. Na caixa de pesquisa na barra de tarefas, digite `gpedit.msc` para executar o editor de Política de Grupo.
3. Navegue para **Política do Computador Local > Configuração do Computador > Modelos Administrativos > Impressoras**.
4. Selecione **Permitir Spooler de Impressão**e permita que ele aceite conexões de clientes.
5. Clique duas vezes na política para abri-la.
6. Selecione **Desativada**.
7. Selecione **OK** para salvar a política.
8. Reinicie o instrumento.

[23] Site da Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Resultado

✓ Executar as etapas acima bloqueará o vetor de ataque remoto, impedindo a entrada de operações remotas de impressão. O sistema não funcionará mais como um servidor de impressão, mas a impressão local em um dispositivo conectado diretamente ainda será possível.

✓ Esta alteração na Política de Grupo definirá a seguinte chave de registro `HKEY_LOCAL_MACHINE\ Software \Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Desative a opção Point and Print no Registro do Windows

Recomendamos que essa tarefa seja realizada por um administrador de TI.

Procedimento

1. Faça login no instrumento.
2. Na caixa de pesquisa na barra de tarefas, digite `regedit` . Em seguida, selecione Editor de Registro.
3. Navegue para `HKEY_LOCAL_MACHINE\SOFTWARE \Policies\Microsoft\Windows NT\Printers`.
4. Se ela existir, expanda o ramo Impressoras e certifique-se de que o grupo PointandPrint não exista.
   NOTA! O ramo Impressoras não existe na configuração de fábrica.
   ⇨ Se o grupo **PointandPrint** existir, verifique as configurações a seguir. Se ele existir, então defina o valor como 0.
   `NoWarningNoElevationOnInstall = 0 ou não existe`
   `UpdatePromptSettings = 0 ou não existe`
5. Reinicie o instrumento.

Vulnerabilitatea derulatorului de imprimare Microsoft Windows CVE-2021-34527

(„PrintNightmare”) Actualizare de securitate cibernetică pentru sistemul de operare Windows 7

ro ■ 24.09.2021

Vulnerabilitatea derulatorului de imprimare Microsoft Windows
CVE-2021-34527

1 Cu privire la actualizare

PrintNightmare este o vulnerabilitate care afectează sistemele de operare Microsoft Windows.

Există o vulnerabilitate la executarea codului la distanță atunci când serviciul Derulator de imprimare Windows efectuează în mod necorespunzător operații de fișiere privilegiate. Dacă cineva exploatează cu succes această vulnerabilitate, poate executa cod arbitrar cu privilegii de sistem. Atacatorul poate instala apoi programe; poate vizualiza, modifica sau șterge date; sau poate crea conturi noi cu drepturi de utilizator complete.[24]

PrintNightmare nu afectează siguranța și performanța niciunuia dintre dispozitivele ZEISS.

Cu toate acestea, ZEISS recomandă actualizarea dispozitivelor cu pachetele de corecție și/sau setările de registry Microsoft, după caz, pentru a asigura securitatea cibernetică continuă. ZEISS a analizat impactul vulnerabilității asupra produselor ZEISS care folosesc sistemul de operare Windows și numai dispozitivele enumerate mai jos necesită actualizarea.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Dezactivați politica grupului privind derulatoarele de imprimare

Este recomandat ca un administrator IT al site-ului să efectueze această sarcină.

Mod de procedare

1. Conectați-vă la instrument.
2. În caseta de căutare de pe bara de activități, tastați `gpedit.msc` pentru a executa editorul de politici de grup.
3. Navigați la **Politică computer local > Configurare computer> Șabloane administrative> Imprimante**.
4. Selectați **Se permite derulator de imprimare** pentru a accepta conexiunile client.
5. Faceți dublu clic pe politică pentru a o deschide.
6. Selectați **Dezactivat**.
7. Selectați **OK** pentru a salva politica.
8. Reporniți instrumentul.

[24] Site-ul web Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Rezultat

- ✓ Efectuarea pașilor de mai sus va bloca vectorul de atac la distanță, prevenind operațiunile de imprimare de la distanță la intrare. Sistemul nu va mai funcționa ca un server de imprimare, dar imprimarea locală pe un dispozitiv atașat direct va fi totuși posibilă.
- ✓ Această modificare a politicii de grup va seta următoarea cheie de registry `HKEY_LOCAL_MACHINE\ Software \Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Dezactivați Punctare și imprimare în Registry Windows

Este recomandat ca această operațiune să fie efectuată de un administrator IT.

Mod de procedare

1. Conectați-vă la instrument.
2. În caseta de căutare de pe bara de activități, tastați `regedit` și selectați Editor de registry.
3. Navigați la `HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows NT\Printers`.
4. Dacă există, extindeți ramura Imprimante și asigurați-vă că grupul Punctare și imprimare nu există.
   INDICAȚIE! Ramura Imprimante nu există în configurația din fabrică.
   - ⇨ Dacă grupul **Punctare și imprimare** există, verificați următoarele setări și, dacă există, setați valoarea la 0.
     `NoWarningNoElevationOnInstall = 0 sau nu există`
     `UpdatePromptSettings = 0 sau nu există`
5. Reporniți instrumentul.

Уязвимость очереди печати Microsoft Windows CVE-2021-34527

("PrintNightmare") Обновление кибербезопасности для ОС Windows 7

ru ■ 24.09.2021

1 Об обновлении

PrintNightmare — уязвимость, затрагивающая операционные системы Microsoft Windows.

Существует уязвимость выполнения удаленного кода, когда служба очереди печати Windows неправильно выполняет операции с привилегированными файлами. Злоумышленник, успешно воспользовавшийся этой уязвимостью, может запустить произвольный код с привилегиями SYSTEM. После этого злоумышленник может устанавливать программы, просматривать, изменять или удалять данные либо создавать новые учетные записи с полными правами пользователя.[25]

PrintNightmare не влияет на безопасность и производительность ни на одном из устройств ZEISS.

Тем не менее, ZEISS рекомендует обновлять устройства с помощью исправления Майкрософт или параметров реестра, если это применимо, чтобы постоянно обеспечивать кибербезопасность. Компания ZEISS проанализировала влияние этой уязвимости на продукты ZEISS под управлением ОС Windows, и только устройства, перечисленные ниже, должны выполнить обновление.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Отключение групповой политики очереди печати

Эту задачу рекомендуется выполнять ИТ-администратору сайта.

Порядок действий

1. Выполните вход в программное обеспечение устройства.
2. В поле поиска на панели задач введите `gpedit.msc` для запуска редактора групповой политики.
3. Перейдите в раздел **Политика "Локальный компьютер > Конфигурация компьютера > Административные шаблоны > Принтеры**.
4. Выберите **Разрешить очереди печати принтера** прием клиентских подключений.
5. Дважды щелкните политику, чтобы открыть ее.
6. Выберите **Отключено**.

[25] Сайт Майкрософт: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

7. Выберите **OK** для сохранения политики.
8. Перезапустите устройство.

Результат

✓ Выполнение описанных шагов блокирует вектор удаленной атаки, предотвращая входящие операции удаленной печати. Система больше не будет функционировать как сервер печати, но локальная печать на непосредственно подключенном устройстве по-прежнему будет возможна.

✓ Это изменение групповой политики установит следующий раздел реестра: `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\RegisterSpoolerRemoteRpcEndPoint = 2`

3 Деактивируйте функцию указания и печати в реестре Windows

Рекомендуется выполнение этой задачи ИТ-администратором.

Порядок действий

1. Выполните вход в программное обеспечение устройства.
2. В поле поиска на панели задач введите `regedit` и выберите Редактор реестра.
3. Перейдите в раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Если он существует, разверните ветвь Printers и убедитесь, что группа PointandPrint отсутствует.
   ПРИМЕЧАНИЕ! Ветвь Printers отсутствует в заводской конфигурации.

   ⇨ Если группа **PointandPrint** существует, проверьте следующие параметры, и если она существует, задайте значение 0.
   `NoWarningNoElevationOnInstall = 0 или "не существует"`
   `UpdatePromptSettings = 0 ил "не существует"`
5. Перезапустите устройство.

Zraniteľnosť zaraďovača tlače systému Microsoft Windows CVE-2021-34527

(„PrintNightmare“) Aktualizácia kybernetickej bezpečnosti pre operačný systém Windows 7

Zraniteľnosť zaraďovača tlače systému
Microsoft Windows CVE-2021-34527

1 Informácie o aktualizácii

PrintNightmare je zraniteľnosť ovplyvňujúca operačné systémy Microsoft Windows (OS).

Zraniteľnosť pri vzdialenom spustení kódu existuje, keď služba zaraďovača tlače systému Windows nesprávne vykonáva privilegované operácie so súbormi. Útočník, ktorý úspešne využil túto zraniteľnosť, môže spustiť ľubovoľný kód so systémovými oprávneniami. Útočník by potom mohol nainštalovať programy; zobraziť, zmeniť alebo odstrániť údaje; alebo vytvárať nové účty s úplnými užívateľskými právami.[26]

PrintNightmare nemá vplyv na bezpečnosť a výkon na žiadnom zariadení spoločnosti ZEISS.

Spoločnosť ZEISS však odporúča aktualizovať zariadenia s nastaveniami opravy a/alebo databázy Registry spoločnosti Microsoft, aby sa zabezpečila trvalá kybernetická bezpečnosť. Spoločnosť ZEISS analyzovala vplyv zraniteľnosti na produkty ZEISS so systémom Windows OS a aktualizáciu musia spustiť iba zariadenia uvedené nižšie.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Vypnutie skupinovej politiky zaraďovača tlače

Odporúča sa, aby túto úlohu vykonal IT správca lokality.

Postup

1. Prihláste sa do prístroja.
2. Do vyhľadávacieho poľa na paneli úloh zadajte `gpedit.msc` a spustite editor skupinovej politiky.
3. Prejdite na možnosť **Lokálna politika počítača > Konfigurácia počítača > Šablóny na správu > Tlačiarne**.
4. Vyberte možnosť **Povoliť zaraďovač tlače**, aby bolo možné prijímať pripojenia klientov.
5. Dvojitým kliknutím na politiku ju otvorte.
6. Vyberte možnosť **Vypnuté**.
7. Ak chcete politiku uložiť, vyberte možnosť **OK**.
8. Reštartujte nástroj.

[26] Webová lokalita spoločnosti Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Výsledok

✓ Vykonaním vyššie uvedených krokov zablokujete vektor vzdialeného útoku tak, že zamedzíte prichádzajúce operácie vzdialenej tlače. Systém už nebude fungovať ako tlačový server, ale lokálna tlač na priamo pripojenom zariadení bude stále možná.

✓ Táto zmena skupinovej politiky nastaví nasledujúci kľúč databázy Registry `HKEY_LOCAL_MACHINE\ Software \Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Deaktivujte službu Point and Print v databáze Registry systému Windows

Odporúčame, aby túto úlohu vykonal správca IT.

Postup

1. Prihláste sa do prístroja.
2. Do vyhľadávacieho poľa na paneli úloh zadajte `regedit`a potom vyberte položku Editor databázy Registry.
3. Prejdite do priečinka `HKEY_LOCAL_MACHINE\SOFTWARE \Policies\Microsoft\Windows NT\Printers`.
4. Ak existuje, rozbaľte vetvu Tlačiarne a uistite sa, že skupina PointandPrint neexistuje.
   UPOZORNENIE! Pri továrenských nastaveniach vetva Tlačiarne neexistuje.
   ⇨ Ak skupina **PointandPrint** existuje, skontrolujte nasledujúce nastavenia, ak existuje, nastavte hodnotu na hodnotu 0 .
   `NoWarningNoElevationOnInstall = 0 alebo neexistuje`
   `UpdatePromptSettings = 0 alebo neexistuje`
5. Reštartujte nástroj.

Ranljivost tiskanja v ozadju sistema Microsoft Windows CVE-2021-34527

(»PrintNightmare«) Posodobitev kibernetske varnosti za OS Windows 7

1 O posodobitvi

PrintNightmare je ranljivost, ki prizadene operacijske sisteme (OS) Microsoft Windows.

Ranljivost izvajanja oddaljene kode obstaja, ko storitev tiskanja v ozadju sistema Windows nepravilno izvede prednostne datotečne operacije. Napadalec, ki uspešno izkoristi to ranljivost, lahko izvede poljubno kodo s SISTEMSKIMI pravicami. Napadalec lahko potem namešča programe, si ogleda podatke, jih spremeni ali izbriše ali pa ustvarja nove račune s polnimi uporabniškimi pravicami.[27]

PrintNightmare ne vpliva na varnost in učinkovitost delovanja nobene naprave ZEISS.

Vendar ZEISS priporoča posodobitev naprav s popravki sistema Microsoft in/ali nastavitvami registra, kot je ustrezno, da se zagotovi nadaljnja kibernetska varnost. ZEISS je analiziral učinek ranljivosti na izdelke ZEISS, v katerih se izvaja OS Windows, in posodobitev je treba izvesti le v napravah, ki so navedene v nadaljevanju.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Onemogočanje pravilnika skupine o tiskanju v ozadju

Priporočamo, da to opravilo izvede skrbnik IT za spletno mesto.

Postopanje

1. Prijavite se v instrument.
2. V iskalno polje v opravilni vrstici vnesite `gpedit.msc`, da zaženete urejevalnik pravilnika skupine.
3. Pomaknite se do možnosti **Pravilnik lokalnega računalnika > Konfiguracija računalnika > Skrbniške predloge > Tiskalniki**.
4. Izberite možnost **Dovoli tiskanje v ozadju**, da sprejmete povezave z odjemalci.
5. Dvokliknite pravilnik, da ga odprete.
6. Izberite **Onemogočeno**.
7. Če želite pravilnik shraniti, izberite **V redu**.
8. Znova zaženite instrument.

[27] Microsoftovo spletno mesto: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Rezultat

✓ Z izvajanjem zgoraj navedenih korakov boste blokirali vektor oddaljenega napada s preprečevanjem dohodnih operacij oddaljenega tiskanja. Sistem ne bo več deloval kot tiskalni strežnik, a bo lokalno tiskanje v neposredno povezano napravo še vedno mogoče.

✓ S to spremembo pravilnika skupine bo nastavljen naslednji registrski ključ `HKEY_LOCAL_MACHINE\ Software \Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`.

3 Deaktiviranje funkcije Pokaži in natisni v registru sistema Windows

Priporočamo, da to opravilo izvede skrbnik IT.

Postopanje

1. Prijavite se v instrument.
2. V iskalno polje v opravilni vrstici vnesite `regedit` in nato izberite urejevalnik registra.
3. Pomaknite se do `HKEY_LOCAL_MACHINE\SOFTWARE \Policies\Microsoft\Windows NT\Printers`.
4. Če veja Tiskalniki obstaja, jo razširite, in se prepričajte, da skupina PointandPrint ne obstaja.
   OPOZORILO! Veja Tiskalniki ne obstaja v tovarniški konfiguraciji.
   ⇨ Če skupina **PointandPrint** obstaja, preverite naslednje nastavitve; če obstaja, nastavite vrednost na 0.
   `NoWarningNoElevationOnInstall = 0 ali ne obstaja`
   `UpdatePromptSettings = 0 ali ne obstaja`
5. Znova zaženite instrument.

Vulnerabilidad de cola de impresión CVE-2021-34527 de Microsoft Windows

("PrintNightmare") Actualización de ciberseguridad para el sistema operativo Windows 7

es ■ 24/09/2021

1 Acerca de la actualización

PrintNightmare es una vulnerabilidad que afecta a los sistemas operativos (SO) Microsoft Windows.

Existe una vulnerabilidad de ejecución remota de código cuando el servicio de cola de impresión en Windows realiza incorrectamente operaciones de archivos con privilegios. Un atacante que aprovechara esta vulnerabilidad podría ejecutar código arbitrario con privilegios de SYSTEM. Por tanto, un atacante podría instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con derechos de usuario absolutos.[28]

PrintNightmare no afecta a la seguridad ni al rendimiento de ninguno de los dispositivos ZEISS.

Sin embargo, ZEISS recomienda actualizar los dispositivos con la configuración de revisiones o registro de Microsoft, según corresponda, para garantizar la ciberseguridad continua. ZEISS ha analizado el impacto de la vulnerabilidad en los productos ZEISS que ejecutan el sistema operativo Windows y solo los dispositivos enumerados a continuación deben ejecutar la actualización.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Deshabilitar la Directiva de grupo de la cola de impresión

Se recomienda que esta tarea la lleve a cabo un administrador de TI del sitio.

Forma de proceder

1. Inicie sesión en el instrumento.
2. En el cuadro de búsqueda de la barra de tareas, escriba `gpedit.msc` para ejecutar el editor de Directivas de grupo.
3. Vaya a **Directiva del equipo local > Configuración de equipos > Plantillas administrativas > Impresoras**.
4. Seleccione **Permitir cola de impresión** para aceptar conexiones de cliente.
5. Haga doble clic en la directiva para abrirla.
6. Seleccione **Deshabilitado**.
7. Seleccione **Aceptar** para guardar la directiva.
8. Reinicie el instrumento.

[28] Sitio web de Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Resultado

✓ Realizar los pasos anteriores bloqueará el vector de ataque remoto al evitar las operaciones de impresión remota entrantes. El sistema ya no funcionará como un servidor de impresión, pero todavía será posible la impresión local en un dispositivo conectado directamente.

✓ Este cambio de la Directiva de grupo establecerá la siguiente clave de registro `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Desactive Point and Print en el Registro de Windows

Se recomienda que esta tarea la realice un administrador de TI.

Forma de proceder

1. Inicie sesión en el instrumento.
2. En el cuadro de búsqueda de la barra de tareas, escriba `regedit` y a continuación, seleccione Editor del Registro.
3. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Si existe, abra la lista Impresoras y asegúrese de que el grupo PointandPrint no existe.
   ¡INDICACIÓN! La lista Impresoras no existe en la configuración de fábrica.
   ⇨ Si el grupo **PointandPrint** existe, compruebe la siguiente configuración y si existe, ajuste el valor a 0.
   `NoWarningNoElevationOnInstall = 0 o no existe`
   `UpdatePromptSettings = 0 o no existe`
5. Reinicie el instrumento.

Vulnerabilidad CVE-2021-34527 localizada en la cola de impresión de Microsoft Windows

("PrintNightmare") Actualización de ciberseguridad para Windows 7 OS

es-LatinAmerica419 ■ 24/9/2021

Vulnerabilidad CVE-2021-34527 localizada en la cola de impresión de Microsoft Windows

1 Acerca de la actualización

PrintNightmare es una vulnerabilidad que afecta los sistemas operativos (operating system, OS) de Microsoft Windows.

Ocurre una vulnerabilidad de ejecución de código remoto cuando el servicio de cola de impresión de Windows realiza incorrectamente operaciones de archivo privilegiadas. Un atacante que aproveche con éxito esta vulnerabilidad podría ejecutar un código arbitrario con privilegios de SISTEMA. El atacante podría, entonces, instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con todos los derechos de usuario.[29]

PrintNightmare no afecta la seguridad ni el rendimiento de ninguno de los dispositivos ZEISS.

Sin embargo, ZEISS recomienda actualizar los dispositivos con el parche de Microsoft o la configuración del registro, según corresponda, para garantizar la ciberseguridad continua. ZEISS ha analizado el impacto de la vulnerabilidad en los productos ZEISS con Windows OS, y solo debe ejecutarse la actualización en los siguientes dispositivos:

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Deshabilitar la directiva de grupo Cola de impresión

Se recomienda que un administrador de TI del centro realice esta tarea.

Procedimiento

1. Inicie sesión en el instrumento.
2. En el cuadro de búsqueda de la barra de tareas, escriba `gpedit.msc` para ejecutar el editor de directivas de grupo.
3. Navegue a **Local Computer Policy > Computer Configuration > Administrative Templates > Printers**.
4. Seleccione **Allow Print Spooler** (Permitir la cola de impresión) para aceptar las conexiones cliente.
5. Haga doble clic en la directiva para abrirla.
6. Seleccione **Disabled** (Deshabilitada).
7. Seleccione **OK** (Aceptar) para guardar la directiva.
8. Reinicie el instrumento.

[29] Sitio web de Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Resultado

- ✓ Los pasos anteriores bloquearán el vector de ataque remoto al impedir las operaciones de impresión remota entrantes. El sistema ya no funcionará como un servidor de impresión, pero seguirá siendo posible la impresión local a un dispositivo conectado directamente.
- ✓ Este cambio en la directiva de grupo establecerá la siguiente clave de registro: `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\RegisterSpoolerRemoteRpcEndPoint = 2`.

3 Desactivar Apuntar e imprimir en el registro de Windows

Se recomienda que un administrador de TI realice esta tarea.

Procedimiento

1. Inicie sesión en el instrumento.
2. En el cuadro de búsqueda de la barra de tareas, escriba `regedit` y seleccione Registry Editor (Editor del registro).
3. Navegue a `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers`.
4. Si existe, expanda la ramificación Printers (Impresoras) y asegúrese de que el grupo PointandPrint (Apuntar e imprimir) no exista.
   INDICACIÓN La ramificación Printers (Impresoras) no existe en la configuración de fábrica.
   - ⇨ Si el grupo **PointandPrint** existe, verifique la siguiente configuración. Si existe, configure el valor en 0 .
     `NoWarningNoElevationOnInstall = 0 or does not exist`
     `UpdatePromptSettings = 0 or does not exist`
5. Reinicie el instrumento.

Microsoft Windows utskriftshanterare, sårbarhet CVE-2021-34527

(”PrintNightmare”) Cybersäkerhetsuppdatering för Windows 7 OS

sv ■ 2021-09-24

1 Om uppdateringen

PrintNightmare är en sårbarhet som berör Microsoft Windows operativsystem (OS).

En sårbarhet för exekvering av fjärrkod finns när Windows utskriftshanterartjänst inkorrekt utför privilegierade filoperationer. Någon som utför en attack och lyckas utnyttja denna sårbarhet skulle kunna köra godtycklig kod med systembehörighet. Attackens utförare skulle sedan kunna installera program; se, ändra eller radera data eller skapa nya konton med fullständig användarbehörighet.[30]

PrintNightmare påverkar inte säkerhet eller prestanda på någon av ZEISS enheter.

ZEISS rekommenderar dock att enheter uppdateras med Microsofts programfix och/eller registerinställningar – beroende på vad som är tillämpligt – för att säkra cybersäkerheten. ZEISS har analyserat sårbarhetens påverkan på ZEISS-produkter som använder Windows OS. Endast enheter som listas nedan behöver uppdateras.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Avaktivera grupprincipen för utskriftshanteraren

Det rekommenderas att en IT-administratör på plats utför denna uppgift.

Åtgärd

1. Logga in på instrumentet.
2. Skriv `gpedit.msc` i sökrutan i aktivitetsfältet för att köra Redigeraren för grupprinciper.
3. Gå in på **Lokal datorprincip > Datorkonfiguration > Administrativa mallar > Skrivare**.
4. Välj **Tillåt utskriftshanterare** för att acceptera klientanslutningar.
5. Dubbelklicka på principen för att öppna den.
6. Välj **Avaktiverad**.
7. Välj **OK** för att spara principen.
8. Starta om instrumentet.

[30] Microsofts webbplats: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Resultat

- ✓ Om ovanstående steg utförs blockeras fjärrattackvektorer genom att hindra inkommande fjärrutskriftsoperationer. Systemet kommer inte längre att fungera som utskriftsserver, men lokala utskrifter på en direkt kopplad enhet är fortfarande möjliga.
- ✓ Denna grupprincipändring ställer in följande registernyckel `HKEY_LOCAL_MACHINE\ Software\Policies \Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Avaktivera Peka och skriv ut i Windows-registret

Vi rekommenderar att en IT-administratör utför denna uppgift.

Åtgärd

1. Logga in på instrumentet.
2. Skriv `regedit` i sökrutan i aktivitetsfältet. Välj därefter Registereditorn.
3. Gå till `HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows NT\Printers`.
4. Om den finns, visa nivån Printers och kontrollera att gruppen PointandPrint inte finns.
   OBSERVERA! Nivån Printers finns inte i fabrikskonfigureringen.
   - ⇨ Om gruppen **PointandPrint** finns, kontrollera följande inställningar. Om inställningen finns ställer du in värdet till 0.
     `NoWarningNoElevationOnInstall = 0 eller finns inte`
     `UpdatePromptSettings = 0 eller finns inte`
5. Starta om instrumentet.

Microsoft Windows Yazdırma Biriktirici Güvenlik Açığı CVE-2021-34527

("PrintNightmare") Windows 7 İşletim Sistemi için Siber Güvenlik Güncellemesi

tr ■ 24.09.2021

Microsoft Windows Yazdırma Biriktirici
Güvenlik Açığı CVE-2021-34527

1 Güncelleme Hakkında

PrintNightmare, Microsoft Windows işletim sistemlerini (OS) etkileyen bir güvenlik açığıdır.

Windows Yazdırma Biriktirici hizmeti doğru olmayan bir şekilde ayrıcalıklı dosya işlemleri gerçekleştirdiğinde söz konusu olan bir uzaktan kod yürütme güvenlik açığı mevcuttur. Bu güvenlik açığından başarılı bir şekilde yararlanan bir saldırgan, SİSTEM ayrıcalıklarıyla rastgele kod çalıştırabilir. Saldırgan daha sonrasında programlar yükleyebilir; verileri görüntüleyebilir, değiştirebilir ya da silebilir; tam kullanıcı haklarına sahip yeni hesaplar oluşturabilir.[31]

PrintNightmare herhangi bir ZEISS cihazının güvenliğini ve performansını etkilemez.

Ancak ZEISS olarak kesintisiz siber güvenliği temin etmek için gerektiği şekilde cihazları Microsoft yaması ve/veya kayıt günlüğü ayarları ile güncellemenizi tavsiye ediyoruz. ZEISS Windows işletim sistemi kullanan ZEISS ürünlerinde güvenlik açığının etkilerini analiz etmiş olup sadece aşağıda listelenen cihazlarda güncellemenin yapılması gereklidir.

- CIRRUS 400/4000
- CIRRUS 500/5000
- CIRRUS Photo 600/800
- ATLAS 9000
- HFA3
- PLEX Elite 9000

2 Yazıcı Biriktirici Grup İlkesini devre dışı bırakın

Bu işlemin bir tesis BT Yöneticisi tarafından gerçekleştirilmesi tavsiye edilir.

Yapılması gerekenler

1. Cihazda oturum açın.
2. Grup İlkesi düzenleyicisini çalıştırmak için görev çubuğundaki arama çubuğuna `gpedit.msc` yazın.
3. **Yerel Bilgisayar İlkesi > Bilgisayar Yapılandırması > Yönetim Şablonları > Yazıcılar** ögesine gidin.
4. İstemci bağlantılarını kabul etmek için **Yazdırma Biriktiricisine İzin Ver** ögesini seçin.
5. Açmak için ilkeye çift tıklayın.
6. **Devre Dışı** ögesini seçin.
7. İlkeyi kaydetmek için **Tamam** düğmesine basın.
8. Cihazı yeniden başlatın.

[31] Microsoft web sitesi: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Sonuç

- ✓ Yukarıdaki adımların gerçekleştirilmesi, gelen uzaktan yazdırma işlemlerini önleyerek uzak saldırı vektörünü engelleyecektir. Sistem artık bir yazdırma sunucusu olarak çalışmayacaktır ancak doğrudan bağlı bir cihaz ile yerel yazdırma işlemi mümkündür.
- ✓ Bu Grup İlkesi şu kayıt defteri anahtarını düzenleyecektir: `HKEY_LOCAL_MACHINE\ Software\Policies \Microsoft\Windows NT\Printers\ RegisterSpoolerRemoteRpcEndPoint = 2`

3 Windows Kayıt Defterinde İşaretle ve Yazdır Özelliğini Devre Dışı Bırakın

Bu işlemin bir BT yöneticisi tarafından gerçekleştirilmesini tavsiye ederiz.

Yapılması gerekenler

1. Cihazda oturum açın.
2. Görev çubuğundaki arama kutusuna `regedit` yazın ve ardından Kayıt Defteri Düzenleyicisini seçin.
3. `HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows NT\Printers` ögesine gidin.
4. Mevcutsa Yazıcılar dalını genişletin ve PointandPrint gurubunun mevcut olmadığından emin olun.
   BİLGİ! Yazıcılar dalı fabrika yapılandırmasında mevcut değildir.
   - ⇨ **PointandPrint** grubu mevcutsa şu ayarları kontrol edin, mevcutsa değerini 0 olarak ayarlayın.
     `NoWarningNoElevationOnInstall = 0 ya da mevcut değil`
     `UpdatePromptSettings = 0 ya da mevcut değil`
5. Cihazı yeniden başlatın.

Carl Zeiss Meditec, Inc.

5300 Central Parkway

Dublin, CA 94568

USA

Toll Free: 1-800-341-6968

Phone: 1–925–557–4100

Fax: 1-925-557-4101

Internet: www.zeiss.com/med

E-Mail: info.meditec@zeiss.com

2660021182725 Rev C 2021-09