Olympus Winter & Ibe GmbH, Kuehnstraße 61, 22045 Hamburg

Aan alle betrokkenen

Datum
30-07-2021

PrintNightmare -
Kwetsbaarheid met uitvoering van externe code in Windows Print Spooler

Geachte mevrouw/meneer,

Er is een kritieke kwetsbaarheid in de Windows Print Spooler-service gedetecteerd. Deze wordt "Print-Nightmare" genoemd. Microsoft heeft aan dit beveiligingslek het nummer **CVE-2021-1675** toegekend.

Op 29 juni 2021 begonnen aanvallen op de kwetsbaarheid te circuleren. Microsoft heeft toen een tweede nummer aan dit beveiligingslek toegekend: **CVE-2021-34527**.

Op 7 juli 2021 heeft Microsoft out-of-band-updates uitgebracht voor sommige (maar niet alle) versies van Windows. Volgens het bijgewerkte advies van Microsoft "bevatten de beveiligingsupdates die op en na 6 juli 2021 zijn uitgebracht bescherming voor CVE-2021-1675 en de extra aanval voor uitvoering van externe code in de Windows Print Spooler-service die bekend staat als "PrintNightmare", gedocumenteerd in CVE-2021 -34527." Misbruik 'in the wild' is gedetecteerd en hierbij zijn ALLE Windows-systemen betrokken.

Op 15 juli 2021 heeft Microsoft een derde nummer toegekend aan de PrintNightmare-kwetsbaarheid: **CVE-2021-34481**. Voor zover bekend heeft er nog geen openbare aanval plaatsgevonden op deze zwakke plek.

Getroffen OSTE-apparaten

Alle versies van de volgende OSTE-producten bevatten een versie van Windows en worden getroffen door de PrintNightmare-kwetsbaarheid:

- VMC-3
- VMC-7
- VMC-10
- VMC-30.

OSTE heeft servicebulletin SBU_100-219-293 uitgebracht om de PrintNightmare-kwetsbaarheid op deze producten aan te pakken. Dit servicebulletin bevat instructies voor servicetechnici over het stoppen en uitschakelen van de Print Spooler-service in Windows voor VMC-3, VMC-7, VMC-10 en VMC-30. Uitschakeling van de Print Spooler-service van Windows is een snelle en effectieve oplossing om de PrintNightmare-kwetsbaarheid in Windows te sluiten.

Neem contact op met de Olympus-service om de herstelacties uit het servicebulletin op uw VMC toe te passen.

Overige OSTE-producten

OSTE produceert en levert ook software, die geïnstalleerd moet worden op computers met Windows als besturingssysteem:

- ENDOBASE
- Hytrack

Vanwege het hoge risico van de PrintNightmare-kwetsbaarheid raadt OSTE ten zeerste aan om de volgende herstelinstructies toe te passen om het risico veroorzaakt door de PrintNightmare-kwetsbaarheid te minimaliseren.

Algemene aanbeveling

Alle Windows-versies en alle typen Windows (clients en serverinstallaties) worden door de PrintNightmare-kwetsbaarheid getroffen.

Als een Windows-computer de afdrukfunctionaliteit niet nodig heeft, raadt OSTE aan om de Print Spooler-service van Windows op deze computers te stoppen en uit te schakelen. Uitschakeling van de Print Spooler-service verhelpt de PrintNightmare-kwetsbaarheid op alle versies en typen van Windows. Hiermee wordt echter ook de mogelijkheid uitgeschakeld om vanaf een computer af te drukken.

De afdrukfunctionaliteit is vereist voor Hytrack-servers als automatisch afdrukken van reprocessingsprotocollen moet worden uitgevoerd en op Hytrack-clients voor handmatig afdrukken van protocollen.

Op ENDOBASE-servers is de afdrukfunctie niet nodig.

Voor het derde CVE-nummer in verband met PrintNightmare – CVE-2021-34481 – is uitschakeling van de Print Spooler-service de enige tijdelijke oplossing die door Microsoft is gegeven op het moment van uitgave van dit document (juli 2021).

Meer informatie vindt u op de Microsoft-webpagina voor CVE-2021-34481:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481

Als afdrukken vanaf een Windows-computer vereist is, hangt de aanbevolen herstelactie af van de betreffende Windows-versie.

Windows 10 en Windows 10-gebaseerde serverversies

Microsoft heeft beveiligingsupdates gepubliceerd voor alle versies van Windows 10 en de bijbehorende serverversies. Gedetailleerde informatie en koppelingen naar de gerelateerde Knowledgebase-artikelen zijn beschikbaar op de Microsoft-webpagina voor CVE-2021-34527:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Naast installatie van de updates moet u, om uw systeem te beveiligen, bevestigen dat de volgende registerinstellingen zijn ingesteld op 0 (nul) of niet zijn gedefinieerd:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
- `NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)`
- `UpdatePromptSettings = 0 (DWORD) or not defined (default setting)`

Als `NoWarningNoElevationOnInstall` is ingesteld op 1, maakt het ontwerp uw systeem kwetsbaar.

Windows 7 en Windows 7-gebaseerde serverversies

Microsoft heeft beveiligingsupdates voor Windows 7 en Windows 7-gebaseerde serverversies alleen gepubliceerd voor klanten met een Extended Support Update (ESU)-contract.

Als uitschakeling van de Print Spooler-service geen optie is, zijn er slechts enkele tijdelijke oplossingen om het risico van de PrintNightmare-kwetsbaarheid te minimaliseren.

Inkomend extern afdrukken uitschakelen via Groepsbeleid

Configureer de instellingen via Groepsbeleid als volgt:

`Computer Configuration / Administrative Templates / Printers`

Schakel de beleidsregel "`Allow Print Spooler to accept client connections`" uit om externe aanvallen te blokkeren.

U moet de Print Spooler-service opnieuw opstarten om het groepsbeleid van kracht te laten worden.

Gedetailleerde informatie vindt u op de Microsoft-webpagina voor CVE-2021-34527:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Installatie van nieuwe printerstuurprogramma's beperken (Point-and-Print-instellingen)

Zonder een geïnstalleerde beveiligingsupdate worden bovendien de volgende instellingen aanbevolen om het risico dat wordt veroorzaakt door de PrintNightmare-kwetsbaarheid te beperken:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
- `NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)`
- `UpdatePromptSettings = 0 (DWORD) or not defined (default setting)`

Als `NoWarningNoElevationOnInstall` is ingesteld op 1, maakt het ontwerp uw systeem kwetsbaar.

Met vriendelijke groet,

Alois Baier
Product Security Manager
R&D | Product Security