Incident Response Notificatie

Zero-day kwetsbaarheid - PrintNightmare

PrintNightmare

Datum: 01/07/2021

Versie: 1.0

bsi ISO/IEC 27001 Information Security Management CERTIFIED

NFIR

Over de kwetsbaarheid

Microsoft heeft recent patches gepubliceerd voor een kwetsbaarheid in de printer services in Windows. Deze kwetsbaarheid heeft het CVE-nummer CVE-2021-1675 gekregen en is in juni opgelost met een update. De kwetsbaarheid zou toestaan dat een aanvaller code uitvoert op elke Windows computer die de print spooler service aan heeft staan. Dit is bij een standaard installatie het geval [1][2].

Omdat er nog geen publieke proof-of-concept code beschikbaar is voor CVE-2021-1675, heeft de Chinese security-groep QiAnXin onderzoek gedaan naar de kwetsbaarheid en een manier gevonden om de print spooler service te misbruiken. Hiervan heeft de groep een video gepubliceerd.

Een andere groep, Sangfor, heeft hierop besloten om een publicatie uit te brengen. Deze groep noemt de gevonden bug PrintNightmare. Deze publicatie bevat technische details en ook een proof-of-concept code. De bevinding van Sangfor bleek een andere kwetsbaarheid te betreffen, waar nog geen patch voor beschikbaar is[3].

Impact

Een aanvaller met toegang tot het netwerk kan op systeemniveau toegang krijgen tot Windows elke computer en server die de print spooler service gebruikt. Dit betekent dat een aanvaller volledige toegang tot het hele Windows domein kan krijgen. Hiervoor is een normaal gebruikersaccount vereist.

Medewerkers van NFIR hebben de kwetsbaarheid succesvol kunnen reproduceren op basis van beschikbare proof-of-concept code. De kwetsbaarheid is inzetbaar om volledige toegang te krijgen tot een Windows Domein.

[1] https://nvd.nist.gov/vuln/detail/CVE-2021-1675
[2] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675
[3] https://www.bleepingcomputer.com/news/security/public-windows-printnightmare-0-day-exploit-allows-domain-takeover/

Mogelijke mitigatie

Twee oplossingsrichtingen worden voorgesteld om de kwetsbaarheid te mitigeren. De eerste is de meest veilige wijze van mitigeren, maar deze vereist dat de printer spooler service compleet uitgeschakeld wordt [4]. Indien dit niet mogelijk is, is de tweede manier de rechten van de map waar de exploit-code gebruik van maakt aanpassen, zodat de beschikbare proof-of-concept code in ieder geval niet werkt. Hieronder wordt per manier beschreven hoe dit uitgevoerd zou kunnen worden:

1) De service kan op individuele systemen gestopt worden met de volgende powershell commando's:

```
Stop-Service -Name Spooler -Force
Set-Service -Name Spooler -StartupType Disabled
```

   Het is ook mogelijk een group-policy in te stellen om de printer spooler service uit te schakelen voor computers in het domein. Dit is aan te raden voor groepen computers die de service niet vereisen.

2) Om de bug te misbruiken wordt gebruik gemaakt van een bepaalde map. Op systemen waar de service niet uitgeschakeld kan worden, is het mogelijk om de schrijfrechten op de map te beperken [5]. Dit kan worden gedaan met de volgende commando's:

```
$Path = "C:\Windows\System32\spool\drivers"
$Acl = Get-Acl $Path
$Ar = New-Object  System.Security.AccessControl.FileSystemAccessRule("System", "Modify", "ContainerInherit, ObjectInherit", "None", "Deny")
$Acl.AddAccessRule($Ar)
Set-Acl $Path $Acl
```

   Let op, dit is geen oplossing voor de kwetsbaarheid, maar voorkomt alleen het bekende misbruik ervan.

> NFIR is niet verantwoordelijk voor eventuele ontstane schade welke het gevolg is van het uitvoeren van de geadviseerde mitigerende maatregelen, elke vorm van mitigerende maatregelen dient altijd te worden uitgevoerd met inachtneming van de specifieke situatie binnen de (getroffen) omgevingen.

[4] https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability
[5] https://blog.truesec.com/2021/06/30/fix-for-printnightmare-cve-2021-1675-exploit-to-keep-your-print-servers-running-while-a-patch-is-not-available/

Vervolgstappen

Het wordt geadviseerd om de Windows systemen in ieder geval up-to-date te houden. Hiermee wordt de originele bug waarschijnlijk verholpen. Het is belangrijk systemen zo veel mogelijk up-to-date te houden om misbruik van kwetsbaarheden te voorkomen. Een indicatie van misbruik kan gevonden worden met het volgende Powershell commando[6]:

```
Get-WinEvent -LogName 'Microsoft-Windows-PrintService/Admin' | Select-String -
InputObject {$_.message} -Pattern 'The print spooler failed to load a plug-in
module'
```

In een artikel van DoublePulsar zijn detectieregels beschikbaar gesteld, die gebruikt kunnen worden in combinatie met Windows Defender. Het is aan te raden deze te gebruiken om misbruik van de kwetsbaarheid te kunnen detecteren. Volg hiervoor de onderstaande link:

- https://doublepulsar.com/zero-day-for-every-supported-windows-os-version-in-the-wild-printnightmare-b3fdb82f840c

Het is belangrijk om de komende dagen meldingen van de gebruikte antivirussoftware extra goed in de gaten te houden en alert te zijn op verdacht gedrag in het netwerk. Het wordt geadviseerd om informatie rondom dit thema goed bij te houden en om snel te handelen wanneer dit nodig blijkt te zijn.

Wat moet uw organisatie doen bij mogelijk misbruik?

Indien uw organisatie het slachtoffer is geworden van een aanval, is het dringende advies om onderzoek uit te laten voeren naar de toedracht, in hoeverre aanvallers mogelijk andere systemen hebben gecompromitteerd en welke informatie mogelijk ongeautoriseerd geraadpleegd is.

1. Koppel indien mogelijk de getroffen systemen los van het netwerk, maar laat deze aanstaan (in verband met eventuele sporen zoals het vluchtige geheugen – RAM);
2. Laat de getroffen systemen forensisch onderzoeken; zorg voor adequate backups
3. Reset uw wachtwoorden en gebruikersgegevens
4. Doe aangifte bij de Politie
5. Overweeg een melding te doen bij de Autoriteit Persoonsgegevens

[6] https://www.rapid7.com/blog/post/2021/06/30/cve-2021-1675-printnightmare-patch-does-not-remediate-vulnerability/

NFIR B.V.
Verlengde Tolweg 2
2517 JV Den Haag
Telefoon: 088 - 323 02 05
info@nfir.nl
https://www.nfir.nl