CYBOTS POWERED BY CYCRAFT

CVE-2021-1675
CVE-2021-34527
PrintNightmare

Cybots Pte Ltd

Cybots is founded by IT and Security veterans with more than 30 years of experience in the field. Cybots MDR services combine security expertise with best-in-class AI to help companies effectively prevent cyber threats. Cybots is the commercial presence of CyCraft in Asia and expanding its presence to the EMEA and North American markets.

CyCraft Technology

CyCraft delivers innovative autonomous security for endpoints, data centers, cloud, and hybrid environments to help small, medium, and large organizations secure their assets and sensitive data via our proactive, intelligent, and adaptive security platform, CyCraft AIR.

CyCraft AIR secures government agencies, police and defense organizations, Fortune Global 500 firms, top banks and financial institutions, critical infrastructure, airlines, telecommunications, hi-tech firms, SMEs, and more by being Fast / Accurate / Simple / Thorough. Everything starts from security.

Recent CVE-2021- 1675 (CVE-2021-34527) Attacks

CyCraft recently observed an attack leveraging the Windows Print Service Vulnerability (CVE-2021-1675). This vulnerability allows attackers to use ordinary user accounts to successfully exploit all Windows platforms, including Windows Server 2019 and Windows 10. Microsoft updated in June, but the update did not fully fix the vulnerability. At the end of June, researchers released a new attack proof of concept. As of July 1, there has been no effective patch update.

On July 1, CyCraft has seen evidence of this exploit being successfully used in the wild as a launching point, leading to lateral movement and other aggressive attacker behavior. The stability and availability of this vulnerability are high. It will soon be exploited by more attackers, including via ransomware, invading the intranet for large-scale attacks in the near future. It is recommended that IT departments immediately implement response planning according to the following mitigation measures.

We recommend that Windows environments update immediately to avoid this vulnerability being further utilized. And currently, while this vulnerability is not fully patched, we recommend further mitigation.

CVE-ID

CVE-2021- 1675

This vulnerability is also known as PrintNightmare and the Print Spooler Bug. Microsoft also recently renamed this new vulnerability CVE-2021-34527. The original CVE-2021- 1675 was patched due to allowing an EoP hole; however, further issues were brought to light that CVE-2021- 1675 could also be used for RCE. This is the vulnerability to which we are referring.

NVD Published Data

June 8, 2021

CVSS

7.8 HIGH (CVSS Version 3.x)

Brief Introduction

Microsoft has not fully patched CVE-2021-1675. As a result, all supported and Extended Security Update versions of Windows OS can be infected by malware installed on endpoints via ordinary user accounts. Attackers could gain domain controller system privileges in minutes.

Affected Versions

Windows Server (2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 20H2) and Windows (7, 8.1, RT 8.1, 10).

Repair Suggestions

Since the vulnerability has not been completely patched, there are still risks. It is recommended that after the implementation of Microsoft's update, further mitigation measures are required to prevent this vulnerability from being exploited.

Mitigation Measures

The temporary mitigation measures provided here are as follows :

1. Turn off the service for endpoints that do not need printer service.

   Disable Spooler service

```
Stop-Service Spooler
REG ADD "HKLM\SYSTEM\ CurrentControlSet \Services\Spooler" /v "Start" /t REG_DWORD /d "4" /f
```

2. Uninstall Print-Services

```
Uninstall-WindowsFeature Print-Services
```

3. Through PowerShell prevent the C:\Windows\System32\spool\drivers directory from being maliciously written to:

```
$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
```

High-Risk Vulnerability

Microsoft issued the CVE-2021-1675 vulnerability on June 8, 2021. Under the authority of existing domain users, attackers could get the domain controller’s system privileges. Causes of this vulnerability in Microsoft Windows Print Spooler service stem from RpcAddPrinterDriverEx not being strict enough, allowing any domain user to register a driver with system execution permissions. This vulnerability not only affects the domain controller but can also affect the full Windows system. Currently, Microsoft's patch KB5003646 will still be attacked by the POC and has not yet been fully patched.

CyCraft 24/7 Continuous Monitoring, Detection and Response

CyCraft monitors global threat intelligence 24/7 and provides early warnings and mitigations for public reference, driving more attention to higher-risk vulnerabilities. Please keep up to date with mitigations and updates concerning this Microsoft vulnerability.

References:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1675
- https://github.com/afwu/PrintNightmare
- https://threatpost.com/poc-exploit-windows-print-spooler-bug/167430/
- https://nvd.nist.gov/vuln/detail/CVE-2021-1675
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

CYBOTS POWERED BY CYCRAFT

Everything Starts From Security