Patch Critical Vulnerability in Windows Servers using DNS Server Role

Summary

Microsoft published a Windows®[1] Update for CVE-2020-1350 on July 14, 2020 to patch a Remote Code Execution (RCE) vulnerability on all Windows Server versions utilizing the DNS server role [1][2][3]. The RCE vulnerability targets the handling of DNS Signature (SIG) Resource Records (RRs). The vulnerability requires a carefully crafted SIG response with a large SIG signature block [4]. Internet-facing Windows Servers with DNS server roles will have significant vulnerability risk and should patch or apply the workaround mitigation as soon as possible.

Affected Windows Server operating systems:

- Windows Server version 2004
- Windows Server version 1909
- Windows Server version 1903
- Windows Server version 1803
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2 (no patch, server should be upgraded)
- Windows Server 2003 (no patch, server should be upgraded)

Mitigation Actions

Apply the CVE-2020-1350 patch immediately on Windows Servers with DNS Server roles. The patch is distributed as part of the Windows Update Monthly Rollup, which should be applied to all Windows Servers, even those not using the DNS Server role [5]. Environments with Windows DNS servers that cannot apply the patch immediately should apply the workaround mitigation instead as soon as possible until the patch can be installed, and then the workaround should be removed after the patch is applied.

Apply Update

Each Windows Server version with updates had unique Microsoft Knowledge Base articles published. Administrators should visit the Microsoft Security Response Center portal for CVE-2020-1350 to identify the appropriate Windows Update and apply it promptly. Applying this patch requires a server reboot [3].

Apply Workaround Mitigation

In the event that an update cannot be applied immediately, the following workaround will prevent the vulnerability from being exploited per Microsoft's recommendation. The workaround configures Windows DNS servers to restrict the size of acceptable DNS message packets over TCP to 65,280 bytes (0xFF00). Applying the workaround requires a restart of the DNS service. Minimal side effects pertaining to typical DNS functionality may occur, as TCP-based DNS response packets larger than the below value (0xFF00) will be dropped until the workaround is removed. Apply the patch as soon as possible and remove the workaround once the patch is applied [2][3].

[1] Microsoft Windows is a registered trademark of Microsoft Corporation.

Registry Key	Registry Value	Value
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters	TcpReceivePacketSize (REG_DWORD)	0xFF00

Launch an elevated PowerShell prompt:

```
Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\DNS\Parameters -Name TcpReceivePacketSize -Type DWord -Value 0xFF00
```

Or

Launch an elevated Command prompt:

```
reg.exe add HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters /v TcpReceivePacketSize /t REG_DWORD /d 0xFF00
```

Restart the DNS service or reboot the DNS server.

Reduce Exposure

In conjunction with applying the Windows Update or the workaround to mitigate this vulnerability, follow best practices to limit the exposure of DNS servers to exploitation. Ensure that internal DNS servers are not accessible from the Internet and ensure that Internet-facing DNS servers are not configured as open resolvers.

Works Cited

[1] Microsoft Security Response Center (2020), Security Update: CVE-2020-1350 Vulnerability in Windows Domain Name System (DNS) Server. [Online] Available at: https://mrsc-blog.microsoft.com/2020/07/14/july-2020-security-update-cve-2020-1350-vulnerability-in-windows-domain-name-system-dns-server/ [Accessed Jul 15, 2020]

[2] Microsoft (2020), KB4569509: Guidance for DNS Server Vulnerability CVE-2020-1350. [Online] Available at: https://support.microsoft.com/en-us/help/4569509/windows-dns-server-remote-code-execution-vulnerability [Accessed Jul 15, 2020]

[3] Microsoft Security Response Center (2020), CVE-2020-1350 Windows DNS Server Remote Code Execution Vulnerability. [Online] Available at: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350 [Accessed Jul 15, 2020]

[4] Check Point Research (2020), SIGRed – Resolving Your Way into Domain Admin: Exploiting a 17 Year-old Bug in Windows DNS Servers. [Online] https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-windows-dns-servers/ [Accessed Jul 15, 2020]

[5] National Security Agency (2019), Cybersecurity Information – Update and Upgrade Software Immediately. [Online] Available at: https://media.defense.gov/2019/Sep/09/2002180319/-1/-1/0/Update/%20Upgrade%20Software%20Immediately.docx/%20-%20Copy.pdf [Accessed Jul 15, 2020]

Disclaimer of Endorsement

Notice

This document was developed in furtherance of NSA's cybersecurity missions including its responsibilities to identify and disseminate threats to National Security Systems and Department of Defense information technologies, and to develop and issue security implementation specifications and cybersecurity mitigations. The information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov