CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-035

Windows DNS Server
Remote Code Execution Vulnerability

July 15, 2020 — v1.1

TLP:WHITE

History:

- *14/07/2020 — v1.0 – Initial publication*
- *15/07/2020 — v1.1 – Additional technical details and references added*

Summary

A remote code execution vulnerability exists in Windows Domain Name System (DNS) servers when they fail to properly handle requests. An attacker who successfully exploited the vulnerability could **run arbitrary code in the context of the Local System Account**. Windows servers that are configured as DNS servers are at risk from this vulnerability [1, 3]. The vulnerability was originally found by Check Point, and dubbed **SIGRed** [4, 5]. It has been present for at least last 17 years.

Technical Details

The vulnerability identified has CVSS score 10 [1]. To exploit the vulnerability, an unauthenticated attacker could send malicious requests to a Windows DNS server. Microsoft considers this to be a **wormable** vulnerability, meaning that it has the potential to spread via malware between vulnerable computers without user interaction [1, 3]. The vulnerability stems from a flaw in Microsoft DNS server implementation and is not the result of a protocol level flaw, so it does not affect any other non-Microsoft DNS server implementations.

The vulnerability involves configuring a domain's NS resource records to point to a malicious name server, and querying the target DNS server for the domain in order to have the latter parse responses from the name server for all subsequent queries related to the domain or its subdomains [4]. Then, an attacker can trigger an integer overflow flaw in the function that parses incoming responses for forwarded queries to send a DNS response that contains a SIG resource record larger than 64KB and induce a *controlled heap-based buffer overflow of roughly 64KB over a small allocated buffer* [4, 5].

Products Affected

The following products are affected [1]:

- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server, version 1903 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)
- Windows Server, version 2004 (Server Core installation)

Recommendations

The update release by Microsoft addresses the vulnerability by modifying how Windows DNS servers handle requests [1].

CERT-EU strongly recommends applying the patches from Microsoft as soon as possible.

Workarounds

Microsoft recommends everyone who runs DNS servers to install the security update as soon as possible. However, if it is not possible to apply the patch right away, Microsoft recommends that the following workaround should be used as soon as possible to protect the affected environment in the time before the update [2].

The following registry modification has been identified as a workaround for this vulnerability:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
TcpReceivePacketSize
Value = 0xFF00
```

Note: The DNS Service needs to be restarted for the registry change to take effect [2].

References

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

[2] https://support.microsoft.com/en-us/help/4569509/windows-dns-server-remote-code-execution-vulnerability

[3] https://msrc-blog.microsoft.com/2020/07/14/july-2020-security-update-cve-2020-1350-vulnerability-in-windows-domain-name-system-dns-server/

[4] https://thehackernews.com/2020/07/windows-dns-server-hacking.html

[5] https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/