Microsoft Urges Customers to Patch Critical Windows TCP/IP Bugs

Threat Bulletins | Feb 09, 2021, 03:28 PM

Microsoft has released a set of fixes affecting Windows TCP/IP implementation that includes two Critical Remote Code Execution (RCE) vulnerabilities (CVE-2021-24074, CVE-2021-24094) and an Important Denial of Service (DoS) vulnerability (CVE-2021-24086).

The three TCP/IP security vulnerabilities impact computers running Windows client and server versions starting with Windows 7 and higher.

According to Microsoft, of the three vulnerabilities, the CVE-2021-24086 flaw is most likely to be exploited for orchestration of denial-of-service attacks that cause a STOP error with a Blue Screen of Death in Windows OS.

The two RCE vulnerabilities are complex which make it difficult to create functional exploits, so they are less likely to be exploited in the short term. However, researchers at Microsoft believe attackers will be able to create DoS exploits much more quickly and expect all three issues might be exploited with a DoS attack shortly after release. Thus, Microsoft recommends customers move quickly to apply Windows security updates as soon as possible. These vulnerabilities result from a flaw in Microsoft's implementation of TCP/IP and affect all Windows versions.

Recommendations:

- It is essential that customers apply Windows updates to address these vulnerabilities as soon as possible.
- If applying the update quickly is not practical, workarounds are detailed below in the CVEs that do not require restarting a server:

CVE-2021-24086

1. Set global reassemblylimit to 0

The following command disables packet reassembly. Any out-of-order packets are dropped. Valid scenarios should not exceed more than 50 out-of-order fragments. We recommend testing prior to updating production systems.

```
Netsh int ipv6 set global reassemblylimit=0
```

Further netsh guidance can be found at netsh.

Impact of workaround

There is a potential for packet loss when discarding out-of-order packets.

How to undo the workaround

To restore to default setting "267748640":

```
Netsh int ipv6 set global reassemblylimit=267748640
```

2. Configure firewall or load balancers to disallow IPv6 UDP fragmentation

CVE-2021-24074

1. Set sourceroutingbehavior to "drop"

Use the following command:

```
netsh int ipv4 set global sourceroutingbehavior=drop
```

For more information about ipv4 registry settings see Additional Registry Settings

Impact of workaround

IPv4 Source routing is considered insecure and is blocked by default in Windows; however, a system will process the request and return an ICMP message denying the request. The workaround will cause the system to drop these requests altogether without any processing.

How to undo the workaround

To restore to default setting "Dontforward":

```
netsh int ipv4 set global sourceroutingbehavior=dontforward
```

2. Configure firewall or load balancers to disallow source routing requests

CVE-2021-24094

1. Set global reassemblylimit to 0

The following command disables packet reassembly. Any out-of-order packets are dropped. Valid scenarios should not exceed more than 50 out-of-order fragments. We recommend testing prior to updating production systems.

```
Netsh int ipv6 set global reassemblylimit=0
```

Further netsh guidance can be found at netsh.

Impact of workaround

There is a potential for packet loss when discarding out-of-order packets.

How to undo the workaround

To restore to default setting "267748640":

```
Netsh int ipv6 set global reassemblylimit=267748640
```

2. Configure firewall or load balancers to disallow IPv6 UDP fragmentation

Sources:

Microsoft: Multiple Security Updates Affecting TCP/IP: CVE-2021-24074, CVE-2021-24094, and CVE-2021-24086

Windows TCP/IP Remote Code Execution Vulnerability: CVE-2021-24074

Windows TCP/IP Remote Code Execution Vulnerability: CVE-2021-24094

Windows TCP/IP Denial of Service Vulnerability: CVE-2021-24086

Bleeping Computer: Microsoft Urges Customers to Patch Critical Windows TCP/IP Bugs
ITNews: Patch Windows to Avoid Denial of Service Attacks: Microsoft

For Questions or Comments: Please email us at toc@h-isac.org

Reference(s)