Security Advisory 2022-003

New Critical Vulnerabilities in Microsoft Products

January 19, 2022 — v1.2

TLP:WHITE

History:

- *14/01/2022 — v1.0 – Initial publication*
- *17/01/2022 — v1.1 – Update about potential issues*
- *19/01/2022 — v1.2 – Update about OOB patches*

Summary

On the 11th of January 2022, Microsoft released a software update to mitigate several vulnerabilities that affect many of its products. Few of them could lead to remote code execution on certain versions of Microsoft Windows and Server [1], Microsoft Exchange Servers, [2, 3, 4] and Microsoft Office, Word, Excel and Sharepoint [5, 6, 7, 8].

No active exploitation of these vulnerabilities is known yet, however, regarding the `CVE-2022-21907` vulnerability, Microsoft said that organisations should prioritise fixing it, because this vulnerability can become wormable – that is – after infection, the virus can spread laterally on the intranet. Also, a proof-of-concept code is already available publicaly [10].

This is why it is generally recommended to **apply the patches as soon as possible**, but please refer to Recommendations section for additional notes.

Technical Details

The critical vulnerabilities include:

- CVE-2022-21907
- CVE-2022-21846
- CVE-2022-21855
- CVE-2022-21969
- CVE-2022-21840
- CVE-2022-21841
- CVE-2022-21842
- CVE-2022-21837

An attacker could use these vulnerabilities to gain access and maintain persistence on the target host.

In particular, the `CVE-2022-21907` vulnerability is related to the HTTP stack (`http.sys`) used in listening mode to handle HTTP requests on Internet Information Services (IIS) servers. The

vulnerability targets the HTTP trailer support feature, which allows a sender to include additional fields in a message to supply metadata, by providing a specially crafted message that can lead to remote code execution. In other words, an attacker would use a specially crafted packet to send to the target server, and the vulnerability would be triggered when the protocol stack processes the data [9].

There is not much detail available at the moment about how the other vulnerabilities could be exploited.

Affected Products

- Microsoft Server 2022
- Microsoft Windows Server 2019 (unaffected by default)
- Microsoft Windows 11
- Microsoft Windows 10 (version 1809, unaffected by default)
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft Office 2013
- Microsoft Office 2016
- Microsoft Office 2019
- Microsoft Word 2013
- Microsoft Excel 2013
- Microsoft Excel 2016
- Microsoft Sharepoint 2013
- Microsoft Sharepoint 2016
- Microsoft Sharepoint 2019

Recommendations

After Microsoft released the first patches, **several issues have been reported regarding the patches for `CVE-2022-21907` vulnerability**. Patching seems to be going without problems for Windows Server 2016 and Windows Server 2012. However, for Windows Server 2012 R2, Windows Server 2019, Windows Server 2022 and Windows 10/11, there are some issues that have been reported:

- The Hyper-V service no longer starts so it is no longer possible to launch the virtual machines.
- Domain controllers restart in loop.
- Issues with VPN connectivity on Windows client

Based on these issues, five patches have been identified as troublesome:

- Windows Server 2012 R2: KB5009624
- Windows Server 2019: KB5009557
- Windows Server 2022: KB5009555
- Windows 10: KB5009543
- Windows 11: KB5009566

In order to fix these issues, Microsoft released a second set of patches called: **emergency out-of-band (OOB) updates**:

> *This update addresses issues related to VPN connectivity, Windows Server Domain Controllers restarting, Virtual Machines start failures, and ReFS-formatted removable media failing to mount.*

All OOB updates released are available for download on the Microsoft Update Catalog, and some of them can also be installed directly through Windows Update as optional updates. If you want to install the emergency fixes through Windows Update, you will have to manually check for updates because they are optional updates and will not install automatically.

If you cannot immediately install today's out-of-band updates, you can still remove the KB5009624, KB5009557, KB5009555, KB5009566, and KB5009543 updates causing these issues. For that, admins can do a rollback or can issue one of the following commands:

- Windows Server 2012 R2: `wusa /uninstall /kb:KB5009624`
- Windows Server 2019: `wusa /uninstall /kb:KB5009557`
- Windows Server 2022: `wusa /uninstall /kb:KB5009555`
- Windows 10: `wusa /uninstall /kb:5009543`
- Windows 11: `wusa /uninstall /kb:5009566`

Exception: On Microsoft Windows Server 2019 and Windows 10 (version 1809), a mitigation is possible for the `CVE-2022-21907` without applying patches:

- Delete the `DWORD` registry value `EnableTrailerSupport` if present under:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters
```

This mitigation only applies to Windows Server 2019 and Windows 10, version 1809 and does not apply to the Windows 20H2 and newer.

Regarding the other vulnerabilities, no issues has been reported so they can safely be applied.

References

[1] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21907

[2] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21846

[3] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21969

[4] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21855

[5] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21840

[6] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21841

[7] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21842

[8] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21837

[9] https://securityonline.info/cve-2022-21907-http-protocol-stack-remote-code-execution-vulnerability/

[10] https://github.com/antx-code/CVE-2022-21907