CERT-EU

Security Advisory 2022-034

Multiple Critical Vulnerabilities in Microsoft Products

May 20, 2022 — v1.2

TLP:WHITE

History:

- *11/05/2022 — v1.0 – Initial publication*
- *17/05/2022 — v1.1 – Updated with information about issues with Domain Controllers*
- *20/05/2022 — v1.2 – Updated about resolved issues with Domain Controllers*

Summary

On May 11th, Microsoft issued May 2022 Patch Tuesday including fixes for three zero-day vulnerabilities and 75 flaws. Among the zero-days, the vulnerability tracked as CVE-2022-26925 [5] is actively exploited in the wild. It is a new NTLM Relay Attack using an LSARPC flaw, allowing an unauthenticated attacker to coerce the domain controller to authenticate to the attacker using NTLM [1]. The two other zero-days are a denial of service vulnerability in Hyper-V, tracked as CVE-2022-22713 [6], and new remote code execution vulnerability in Azure Synapse and Azure Data Factory, tracked as CVE-2022-29972 [7] and presented in CERT-EU Security Advisory 2022-033 [2].

Out of the 75 flaws, eight are classified as **Critical**, allowing remote code execution or elevation of privilege. These vulnerabilities affect a lot of different Microsoft components, including Excel, Windows LDAP, Remote Desktop Protocol, LSA and others [1].

Bleepingcomputer released a full report, listing all the vulnerabilites assessed by Microsoft Security Updates, and giving a description of each vulnerability and also the systems that it affects [3].

On May 13, additional information became available about authentication issues followed by the installation of the patches on Domain Controller servers. However, on May 19, the issue related to authentication failures of Domain Controlers was resolved in out-of-band updates [12]. Please see the Recommendations section of this advisory for details.

Technical Details

Few technical details have been released by Microsoft. We refer the interested readers to the sources in the references [1-7].

Affected products

The list of affected products is following:

- .NET and Visual Studio
- .NET Framework
- Azure SHIR
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Local Security Authority Server (lsasrv)
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Windows ALPC
- Remote Desktop Client
- Role: Windows Fax Service
- Role: Windows Hyper-V
- Self-hosted Integration Runtime
- Tablet Windows User Interface
- Visual Studio
- Visual Studio Code
- Windows Active Directory
- Windows Address Book
- Windows Authentication Methods
- Windows BitLocker
- Windows Cluster Shared Volume (CSV)
- Windows Failover Cluster Automation Server
- Windows Kerberos
- Windows Kernel
- Windows LDAP - Lightweight Directory Access Protocol
- Windows Media
- Windows Network File System
- Windows NTFS
- Windows Point-to-Point Tunnelling Protocol
- Windows Print Spooler Components
- Windows Push Notifications
- Windows Remote Access Connection Manager
- Windows Remote Desktop
- Windows Remote Procedure Call Runtime
- Windows Server Service
- Windows Storage Spaces Controller
- Windows WLAN Auto Config Service

Recommendations

Microsoft strongly recommends to install security updates as soon as possible on client Windows devices and non-Domain Controller Windows Servers.

On May 13, CISA warned not to install May Windows update on domain controllers, because it might create authentication failures on the server or client for some services [8]. The patches for the two elevations privilege vulnerabilites in Windows Kerberos and Active Directory Domain Services, respectively tracked as CVE-2022-26931 and CVE-2022-26923, are responsible for this service authentication problems once deployed on Windows Server Domain Controlers [9]. However, CISA noted that the application of the updates released by Microsoft will not cause issues on Windows client and non-domain controller server [8].

According to Microsoft, however, regarding Windows Server Domain Controlers, if the patch has been applied, Microsoft recommends to manually map the certificates to a machine account in Active Directory [10, 11]. This is needed until Microsoft issues an official update to address this services authentication problems caused by the security update.

On May 19, Microsoft resolved the issue in out-of-band updates for installation on Domain Controllers. There is no action needed on the client side to resolve authentication issue of Domain Controllers. If you used any workaround or mitigation for this issue, they are no longer needed, and Microsoft recommends you to remove them [12].

Additionally, regarding CVE-2022-26925, Microsoft recommends to read the PetitPotam NTLM relay advisory [4] to have information on how to mitigate these types of attacks.

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2022-patch-tuesday-fixes-3-zero-days-75-flaws/

[2] https://media.cert.europa.eu/static/SecurityAdvisories/2022/CERT-EU-SA2022-033.pdf

[3] https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/May-2022.html

[4] https://msrc.microsoft.com/update-guide/vulnerability/ADV210003

[5] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26925

[6] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22713

[7] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-29972

[8] https://www.cisa.gov/uscert/ncas/current-activity/2022/05/13/cisa-temporarily-removes-cve-2022-26925-known-exploited

[9] https://www.bleepingcomputer.com/news/security/cisa-warns-not-to-install-may-windows-updates-on-domain-controllers

[10] https://docs.microsoft.com/en-us/windows/release-health/status-windows-11-21h2#you-might-see-authentication-failures-on-the-server-or-client-for-services

[11] https://support.microsoft.com/en-gb/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16

[12] https://docs.microsoft.com/en-us/windows/release-health/status-windows-10-21h2#2826msgdesc