10 years CERT-EU

Security Advisory 2022-050

Multiple Critical Vulnerabilities in Microsoft Products

July 14, 2022 — v1.0

TLP:WHITE

History:

- *14/07/2022 — v1.0 – Initial publication*

Summary

On the 12th of July, Microsoft released July's 2022 Patch Tuesday including fixes for one actively exploited zero-day vulnerability and a total of 84 flaws. A zero-day vulnerability tracked as CVE-2022-22047 concerns a Windows CSRSS elevation of privilege, allowing an attacker to gain SYSTEM privileges [1].

Out of the 84 other security flows, four of them are classified as *Critical*, as they allow remote code execution. These critical vulnerabilities affect Microsoft Graphics Component, Windows Network File System and Windows Remote Procedure Call. They are tracked as CVE-2022-22029, CVE-2022-22039, CVE-2022-22038 and CVE-2022-30221 [1].

Bleeping Computer released a full report, listing all the vulnerabilities assessed by Microsoft Security Updates, and giving a description of each vulnerability and also the systems that it affects [2].

Technical Details

Few technical details have been released by Microsoft. We refer the interested readers to the sources in the references [1-13].

Affected Products

The list of affected products is the following:

- AMD CPU Branch
- Azure Site Recovery
- Azure Storage Library
- Microsoft Defender for Endpoint
- Microsoft Edge (Chromium-based)
- Microsoft Graphics Component
- Microsoft Office
- Open Source Software

- Role: DNS Server
- Role: Windows Fax Service
- Role: Windows Hyper-V
- Skype for Business and Microsoft Lync
- Windows Active Directory
- Windows Advanced Local Procedure Call
- Windows BitLocker
- Windows Boot Manager
- Windows Client/Server Runtime Subsystem
- Windows Connected Devices Platform Service
- Windows Credential Guard
- Windows Fast FAT Driver
- Windows Fax and Scan Service
- Windows Group Policy
- Windows IIS
- Windows Kernel
- Windows Media
- Windows Network File System
- Windows Performance Counters
- Windows Point-to-Point Tunneling Protocol
- Windows Portable Device Enumerator Service
- Windows Print Spooler Components
- Windows Remote Procedure Call Runtime
- Windows Security Account Manager
- Windows Server Service
- Windows Shell
- Windows Storage

Recommendations

Microsoft strongly recommends to install security updates as soon as possible.

Mitigation for CVE-2022-22029

Microsoft provided a specific mitigation for CVE-2022-22029, regarding Windows Network File System (NFS) Remote Code Execution Vulnerability. This vulnerability cannot be exploited in NFSV4.1, so in order to mitigate it, Microsoft advises to disable NFSV3, to avoid the attacker exploiting this vulnerability. Microsoft provides the technical details on how to deactivate NFSV3 on the article related to the vulnerability [13].

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2022-patch-tuesday-fixes-exploited-zero-day-84-flaws/

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

[3] https://support.microsoft.com/help/5015807

[4] https://support.microsoft.com/help/5015808

[5] https://support.microsoft.com/help/5015811

[6] https://support.microsoft.com/help/5015814

[7] https://support.microsoft.com/help/5015827

[8] https://support.microsoft.com/help/5015832

[9] https://support.microsoft.com/help/5015863

[10] https://support.microsoft.com/help/5015874

[11] https://support.microsoft.com/help/5015875

[12] https://support.microsoft.com/help/5015877

[13] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22029