Security Advisory 2022-064

Multiple Critical Vulnerabilities in Microsoft Products

September 14, 2022 — v1.0

TLP:WHITE

History:

- *14/09/2022 — v1.0 – Initial publication*

Summary

On the 13th of September, Microsoft released its September 2022 Patch Tuesday advisory including fixes for 2 zero-day vulnerabilities identified `CVE-2022-37969` and `CVE-2022-23960` which affect several Windows system versions.

The patch also contains fixes for five critical vulnerabilities affecting Microsoft Dynamics, Windows IKE Extension and Windows TCP/IP [3,4,5,6,7].

It is highly recommended to patch the affected devices.

Technical Details

CVE-2022-34722 and CVE-2022-34721 - Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability

An unauthenticated attacker could send a specially crafted IP packet to a target machine that is running Windows and has IPSec enabled, which could lead to a remote code execution exploitation. This vulnerability only impacts IKEv1. IKEv2 is not impacted. However, all Windows Servers are affected because they accept both V1 and V2 packets [4,5].

CVE-2022-34718 - Windows TCP/IP Remote Code Execution Vulnerability

An unauthenticated attacker could send a specially crafted IPv6 packet to a Windows node where IPSec is enabled, which could lead to a remote code execution exploitation on that machine [3].

CVE-2022-35805 and CVE-2022-34700 - Microsoft Dynamics CRM (on-premises) Remote Code Execution Vulnerability

An authenticated user could run a specially crafted trusted solution package to execute arbitrary SQL commands. From there, the attacker could escalate and execute commands as `db_owner` within their Dynamics 365 database [6,7].

Products Affected

Global list of affected products by all the vulnerabilities in the September advisory [1]:

- .NET and Visual Studio
- .NET Framework
- Azure Arc
- Cache Speculation
- HTTP.sys
- Microsoft Dynamics
- Microsoft Edge (Chromium-based)
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft Windows ALPC
- Microsoft Windows Codecs Library
- Network Device Enrollment Service (NDES)
- Role: DNS Server
- Role: Windows Fax Service
- SPNEGO Extended Negotiation
- Visual Studio Code
- Windows Common Log File System Driver
- Windows Credential Roaming Service
- Windows Defender
- Windows Distributed File System (DFS)
- Windows DPAPI (Data Protection Application Programming Interface)
- Windows Enterprise App Management
- Windows Event Tracing
- Windows Group Policy
- Windows IKE Extension
- Windows Kerberos
- Windows Kernel
- Windows LDAP - Lightweight Directory Access Protocol
- Windows ODBC Driver
- Windows OLE
- Windows Photo Import API
- Windows Print Spooler Components
- Windows Remote Access Connection Manager
- Windows Remote Procedure Call
- Windows TCP/IP
- Windows Transport Security Layer (TLS)

Recommendations

CERT-EU strongly recommends applying the latest Security Updates as soon as possible [2].

References

[1] https://msrc.microsoft.com/update-guide/releaseNote/2022-Sep

[2] https://msrc.microsoft.com/update-guide/deployments

[3] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-34718

[4] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-34721

[5] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-34722

[6] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-34700

[7] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-35805