Security Advisory 2023-097

Critical Vulnerabilities in Microsoft Products

December 19, 2023 — v1.0

TLP:CLEAR

History:

- *19/12/2023 — v1.0 – Initial publication*

Summary

On December 12, 2023, Microsoft released the December 2023 Patch Tuesday which includes security updates for a total of 35 flaws. Among the vulnerabilities, four were rated as critical [1].

It is recommended updating affected products as soon as possible.

Technical Details

The vulnerabilities `CVE-2023-35630` and `CVE-2023-35641` [2,3], both with a CVSS score of 8.8, affect the Windows Internet Connection Sharing (ICS). Internet Connection Sharing (ICS) is a Windows service that enables one Internet-connected computer to share its Internet connection with other computers on a local area network (LAN). By sending maliciously crafted DHCP messages to a server that runs the ICS service, an attacker could achieve remote code execution.

The vulnerability `CVE-2023-36019` [4], with a CVSS score of 9.6, affects Microsoft Power Platform Connector. A Power Platform connector is a proxy or a wrapper around an API that allows the underlying service to talk to Microsoft Power Automate, Microsoft Power Apps, and Azure Logic Apps. An attacker could manipulate a malicious link, application, or file to disguise it as a legitimate link or file to trick the victim.

The vulnerability `CVE-2023-35628` [5], with a CVSS score of 8.1, affects the Windows MSHTML component. To exploit this vulnerability, an attacker would send a malicious link to the victim via email, or convince the user to click the link, typically by way of an enticement in an email or Instant Messenger message. In the worst-case email attack scenario, an attacker could send a specially crafted email to the user without a requirement that the victim open, read, or click on the link. This could result in the attacker executing remote code on the victim's machine. When using the preview pane, the attacker could exploit this vulnerability by sending a specially crafted email which triggers automatically when it is retrieved and processed by the Outlook client. This could lead to exploitation before the email is viewed in the Preview Pane. Successful exploitation of this vulnerability would rely upon complex memory shaping techniques to attempt an attack.

Affected Products

The vulnerabilities affect Microsoft Windows products:

- Windows Server
- Windows Client
- Azure
- Microsoft Office
- Microsoft Edge
- Microsoft 365

For more information about specific versions, please refer to the Microsoft advisory [6].

Recommendations

It is recommended updating affected products as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2023-patch-tuesday-fixes-34-flaws-1-zero-day/

[2] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-35630

[3] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-35641

[4] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36019

[5] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-35628

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