Security Advisory 2023-077

Microsoft October 2023 Patch Tuesday

October 11, 2023 — v1.0

TLP:CLEAR

History:

- *11/10/2023 — v1.0 – Initial publication*

Summary

Microsoft has released its October 2023 Patch Tuesday Security Updates, addressing a total of 103 CVEs among which 12 are rated as critical, and 91 are rated as important. Microsoft also reported that two vulnerabilities are actively exploited [1,8].

Technical Details

This month's patches fix two vulnerabilities that are known to be actively exploited in the wild:

- **CVE-2023-36563 (CVSS 6.5) - Microsoft WordPad Information Disclosure Vulnerability** [2];

Microsoft has fixed an actively exploited information disclosure vulnerability. An unauthenticated, remote attacker could exploit this vulnerability using social engineering in order to convince a target to open a link or download a malicious file and run it on the vulnerable system. Exploiting this vulnerability could allow the disclosure of NTLM hashes.

- **CVE-2023-41763 (CVSS 5.3) - Skype for Business Elevation of Privilege Vulnerability** [3];

Microsoft has fixed an actively exploited privilege escalation vulnerability. An attacker could make a specially crafted network call to the target Skype for Business server, which could cause the parsing of an http request made to an arbitrary address. This could disclose IP addresses or port numbers or both to the attacker.

Microsoft also provides fixes for the following interesting vulnerabilities:

- **CVE-2023-36434 (CVSS 9.8) - Windows IIS Server Elevation of Privilege Vulnerability** [4];

Microsoft has fixed a remote privilege escalation vulnerability. In a network-based attack, an attacker could brute force user account passwords to log in as that user. Microsoft encourages the use of strong passwords that are more difficult for an attacker to brute force.

- **CVE-2023-35349 (CVSS 9.8) - Microsoft Message Queuing Remote Code Execution Vulnerability** [5];

Microsoft has fixed a remote code execution vulnerability. An unauthenticated, remote attacker could exploit this vulnerability by sending a specially crafted packet to a vulnerable target. In order for a system to be vulnerable to these vulnerabilities, the MSMQ service must be added and enabled. According to Microsoft, if the service is enabled on a Windows installation, a service named "Message Queueing" will be running on TCP port 1801.

- **CVE-2023-36569 (CVSS 8.4) - Microsoft Office Elevation of Privilege Vulnerability** [6];

Microsoft has fixed a privilege escalation vulnerability. Successful exploitation of this vulnerability would provide an attacker with SYSTEM level privileges.

- **CVE-2023-36778 (CVSS 8.0) - Microsoft Exchange Server Remote Code Execution Vulnerability** [7];

Microsoft has fixed a remote code execution vulnerability. A local, authenticated attacker could exploit this vulnerability through a remote PowerShell session with the target server. The vulnerability is caused by improper validation of cmdlet arguments within Microsoft Exchange Server.

Affected Products

These vulnerabilities affect the Microsoft products (Windows OS, Azure Cloud, Office products, etc.)

Note: Microsoft announced that Windows Server 2012 and Windows Server 2012 R2 has reached its end of life as of October 10, 2023. This means that users of these versions of Windows Server will no longer receive security updates [9].

Recommendations

It is recommended applying the security updates as soon as possible to protect systems against potential exploitation, prioritising public facing devices and critical applications.

It is also recommended upgrading systems running Windows Server 2012 or Windows Server 2012 R2 to a supported version as soon as possible.

References

[1] https://msrc.microsoft.com/update-guide/releaseNote/2023-Oct

[2] https://msrc.microsoft.com/update-guide/en-en/advisory/CVE-2023-36563

[3] https://msrc.microsoft.com/update-guide/en-en/advisory/CVE-2023-41763

[4] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-36434

[5] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-35349

[6] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-36569

[7] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-36778

[8] https://www.tenable.com/blog/microsofts-october-2023-patch-tuesday-addresses-103-cves-cve-2023-36563-cve-2023-41763

[9] https://learn.microsoft.com/en-us/lifecycle/announcements/windows-server-2012-r2-end-of-support