Security Advisory 2023-039

Microsoft June Patch Tuesday

September 28, 2023 — v1.1

TLP:CLEAR

History:

- *13/06/2023 — v1.0 – Initial publication*
- *28/09/2023 — v1.1 – Exploit-chain for Microsoft Sharepoint released*

Summary

Microsoft's June 2023 Patch Tuesday includes security updates for more than 70 flaws, including multiple critical vulnerabilities [1].

Update On September 25, STAR Labs researcher published a blog post outlining the successful chaining of CVE-2023-29357 and CVE-2023-24955 to achieve remote code execution (RCE) against Microsoft SharePoint Server. The exploit chain was demonstrated at the Zero Day Initiative's (ZDI) Pwn2Own contest held in Vancouver in March [2,3]. Moreover, On September 26, a proof-of-concept (PoC) for the exploit chain was released on GitHub [4].

It is recommended to apply patches as soon as possible.

Technical details

The key vulnerabilities resolved in this update include:

- CVE-2023-29357 - CVSS 3.1: **9.8** - Microsoft SharePoint Server Elevation of Privilege Vulnerability: This flaw allows an unauthenticated attacker who successfully exploits this vulnerability to gain administrator privileges on the platform.
- CVE-2023-32031 - CVSS 3.1: **8.8** - Microsoft Exchange vulnerability: An authenticated attacker could target server accounts for arbitrary or remote code execution. As an authenticated user, an attacker could attempt to trigger malicious code in the context of the server's account through a network call.
- Microsoft Office vulnerabilities: These flaws allowed threat actors to use maliciously crafted Excel and OneNote documents to perform remote code execution. The vulnerabilities are tracked as CVE-2023-32029 (Excel), CVE-2023-33133 (Excel), CVE-2023-33137 (Excel), CVE-2023-33140 (OneNote), CVE-2023-33131 (Outlook).

Update The exploit chain leverages two vulnerabilities to achieve pre-auth remote code execution (RCE) on the SharePoint server:

- CVE-2023-29357 is an elevation of privilege (EoP) vulnerability in Microsoft SharePoint Server that was assigned a CVSSv3 score of 9.8 and rated critical. A remote, unauthenticated attacker can exploit the vulnerability by sending a spoofed JSON Web Token (JWT) authentication token to a vulnerable server giving them the privileges of an authenticated user on the target. According to Microsoft's advisory, no user interaction is required in order for an attacker to exploit this flaw. This vulnerability was patched during Microsoft's June 2023 Patch Tuesday release [3].

- CVE-2023-24955 is a RCE vulnerability affecting Microsoft SharePoint Server. The vulnerability was assigned a CVSSv3 score of 7.2 and could allow an authenticated Site Owner to execute code on an affected SharePoint Server. This RCE was patched as part of the May 2023 Patch Tuesday release [3].

Affected Products

- Microsoft SharePoint Server
- Microsoft Exchange Server
- Microsoft Office (specifically Excel, OneNote, and Outlook)

Recommendations

Users and administrators are urged to review Microsoft's updates and apply necessary patches immediately to secure their systems.

References

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

[2] https://starlabs.sg/blog/2023/09-sharepoint-pre-auth-rce-chain/

[3] https://www.tenable.com/blog/cve-2023-29357-cve-2023-24955-exploit-chain-released-for-microsoft-sharepoint-server

[4] https://github.com/Chocapikk/CVE-2023-29357