KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft Patch Tuesday Oct 2022

Tracker ID: TN1014 **Date:** 14/October/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Microsoft has issued Patch Tuesday for October 2022, which includes patches for an actively exploited Windows vulnerability along with 84 additional issues. Thirteen critical vulnerabilities that allow privilege elevation, spoofing or remote code execution have been addressed, rendering them one of the most severe vulnerabilities. Sadly, this fix does not address two previously disclosed and widely exploited ProxyNotShell vulnerabilities, CVE-2022-41040 and CVE-2022-41082.

Apart from the twelve vulnerabilities fixed in Microsoft Edge on October 3rd, the patch contains fixes for 39 Elevation of Privilege vulnerabilities, 2 Security Feature Bypass vulnerabilities, 20 Remote Code Execution vulnerabilities, 11 Information Disclosure vulnerabilities, 8 Denial of Service vulnerabilities, and 4 Spoofing vulnerabilities.

This month's Patch Tuesday resolves two publicly disclosed zero-day vulnerabilities. CVE-2022-41033 is an actively exploited Elevation of Privilege vulnerability affecting the Windows COM+ Event System that has been addressed. An attacker who successfully exploits this vulnerability may get unauthorized access to the system. The other CVE-2022-41043 is an Information Disclosure Vulnerability in Microsoft Office. Attackers could use this flaw to acquire access to users' authentication tokens.

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-41040	High	8.8
CVE-2022-41082	High	8.8
CVE-2022-41033	High	7.8
CVE-2022-41043	Low	3.3

Affected Products and Versions

CVE-2022-41033: Windows Server 2012 and 2008 and Windows version 10 and 11

CVE-2022-41043: Microsoft Office LTSC for Mac 2021 and Microsoft Office 2019 for Mac

CVE-2022-41040: Microsoft Exchange Server 2016

CVE-2022-41082: Microsoft Exchange Server 2013, 2016 and 2019.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft Patch Tuesday Oct 2022

Tracker ID: TN1014 **Date:** 14/October/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Recommendations

- Immediately identify the vulnerable instances and apply the vendor-provided fixes as soon as possible.
- Monitor the services and critical assets exposed to the Internet. Collect and review relevant logs, data, and artifacts to identify any threat in the network.

References

- MSRC, Customer Guidance, Security Update Guide, Vulnerabilities, Microsoft, 11th October 2022, External Link (msrc.microsoft.com).
- Lawrence Abrams, Microsoft October 2022 Patch Tuesday fixes zero-day used in attacks, 84 flaws, Bleeping Computer, 11th October 2022, External Link (www.bleepingcomputer.com).
- Tara Seals, Microsoft Addresses Zero-Days, but Exchange Server Exploit Chain Remains Unpatched, Dark Reading, 12th October 2022, External Link (www.darkreading.com).
- NIST, CVE-2022-41033 Detail, 11th October 2022, External Link (nvd.nist.gov).
- NIST, CVE-2022-41043 Detail, 11th October 2022, External Link (nvd.nist.gov).
- NIST, CVE-2022-41040 Detail, 11th October 2022, External Link (nvd.nist.gov).
- NIST, CVE-2022-41082 Detail, 11th October 2022, External Link (nvd.nist.gov).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471