KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft September 2022 Patch Tuesday fixes 64 flaws

Tracker ID: TN0918 **Date:** 16/Sep/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Microsoft's September 2022 Patch Tuesday patched 64 new security flaws, including two zero-days, one of which is actively used in malicious attacks. In terms of severity, 5 of the 64 vulnerabilities are classified as "critical," 57 as "important," 1 as "moderate," and 1 as "low." It addressed 30 remote code execution vulnerabilities, 7 information disclosure vulnerabilities, 18 elevation of privilege vulnerabilities, 1 security feature bypass vulnerability, and 7 denial of service vulnerabilities. The updates follow the patching of 16 vulnerabilities in Microsoft's Chromium-based Edge browser earlier this month.

The actively exploited vulnerability, CVE-2022-37969, has a CVSS score of 7.8 and is a privilege escalation vulnerability flaw affecting the Windows Common Log File System (CLFS) Driver that an adversary could exploit to gain SYSTEM rights on an already compromised asset. An attacker must already have access to the target system to execute code on it. This approach does not deliver RCE if the attacker does not already have that capability on the target system. Another zero-day, CVE-2022-23960, also known as Branch History Injection or Spectre-BHB, which affects only ARM64-based systems, has also been patched; however, a CVSS score is yet to be issued.

Other notable vulnerabilities include CVE-2022-34718, a remote code execution vulnerability in Windows TCP/IP with a CVSS score of 9.8. It is possible to exploit it by sending a specially designed IPv6 packet to a Windows node with IPsec enabled, allowing a remote, unauthenticated attacker to execute code with elevated privileges on vulnerable systems without user interaction. Only systems with IPv6 enabled and IPsec configured are affected. This vulnerability could be exploited by attacks on supply chains that use an IPsec tunnel to connect contractor and client networks.

CVE-2022-34721 and CVE-2022-34722, both with a 9.8 CVSS score and affecting the Windows Internet Key Exchange (IKE) Protocol Extensions, were also patched as they could allow an unauthenticated attacker to send a specially designed IP packet to a target computer running Windows and equipped with IPSec, enabling RCE. CVE-2022-34700 and CVE-2022-35805, both with CVSS 8.8, affect Dynamics 365 (On-Premises) and may allow an authenticated user to perform SQL injection attacks and execute commands as the database owner within their Dynamics 356 database.

CVE-2022-38005, with a CVSS score of 7.8, is an elevation of privilege vulnerability in the Print Spooler module that can be exploited to get system-level rights. CVE-2022-34724, with a CVSS score of 7.5, is a denial-of-service weakness in the Windows DNS server that a remote, unauthenticated attacker could exploit to disrupt the DNS service required to access websites and cloud resources. Microsoft also fixed 5 privilege escalation weaknesses in Windows Kerberos and Kernel, as well as 15 remote code execution flaws in the Microsoft ODBC Driver, OLE DB Provider for SQL Server, and SharePoint Server. We advise enterprises to install the updates as soon as feasible to avoid exploitation.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft September 2022 Patch Tuesday fixes 64 flaws

Analysis

Below is the list of few important CVEs released in Patch Tuesday.

CVE ID	Severity	CVSS Score
CVE-2022-34718	Critical	9.8
CVE-2022-34721	Critical	9.8
CVE-2022-34722	Critical	9.8
CVE-2022-34700	High	8.8
CVE-2022-35805	High	8.8
CVE-2022-34724	High	7.5
CVE-2022-37969	High	7.8
CVE-2022-38005	High	7.8
CVE-2022-23960	N/A	N/A

Affected Products and Versions

- For CVE-2022-34718, CVE-2022-34721, CVE-2022-34722, CVE-2022-37969 and CVE-2022-38005 the following products are affected:
    - All Windows 7, 8, 10 versions.
    - All windows servers are affected.
- CVE-2022-34700 and CVE-2022-35805: Affects only Microsoft Dynamics CRM (on-premises) 9.1, and 9.0.
- CVE-2022-34724: All Windows Servers are affected.
- CVE-2022-23960: Affects ARM64-based systems.

Recommendations

- Immediately identify the vulnerable instances and apply the vendor-provided patches as soon as possible.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft September 2022 Patch Tuesday fixes 64 flaws

References

- Security Update Guide: Please apply filter for September, Microsoft, 13th September 2022, External Link (msrc.microsoft.com)
- Ravie Lakshmanan, Microsoft's Latest Security Update Fixes 64 New Flaws, Including a Zero-Day, Hacker News, 13th September 2022, External Link (thehackernews.com)
- Lawrence Abrams, Microsoft September 2022 Patch Tuesday fixes zero-day used in attacks, 63 flaws. Bleeping Computer, 13th September 2022, External Link (bleepingcomputer.com)
- Tara Seals, Microsoft Quashes Actively Exploited Zero-Day, Wormable Critical Bugs, Dark Reading, 13th September 2022, External Link (darkreading.com)
- Renato Marinho, Microsoft September 2022 Patch Tuesday, SANS , 13th September 2022, External Link (isc.sans.edu)

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

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia