KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft Patch Tuesday Mar 2023 - Fixes Two Exploited Zero-Days

Tracker ID: TN2343 **Date:** March 16, 2023 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Microsoft's March 2023 Patch Tuesday release addressed a collection of 80 security flaws, two of which have been actively exploited in the wild. Eight of the 80 vulnerabilities are classified as Critical, 71 as Important, and one as Moderate. The patches come on top of the 29 issues fixed in Microsoft's Chromium-based Edge browser in over the last week. The two actively exploited vulnerabilities are a Microsoft Outlook privilege escalation issue tracked as CVE-2023-23397 with a CVSS score of 9.8 and a Windows SmartScreen security feature bypass recorded as CVE-2023-24880 with a CVSS score of 5.1.

CVE-2023-23397 is a Microsoft Outlook vulnerability that could allow a remote attacker to acquire elevated privileges on the affected machine. This vulnerability exists in Microsoft Outlook since the programme leaks the Net-NTLMv2 hash of a user's account, which could serve as the foundation of an NTLM Relay attack against another service to authenticate as the user. An attacker could send specially crafted email that automatically triggers when it is retrieved and processed by the email server. This may result in exploitation before the email is displayed in the preview pane. Thus, a remote attacker could obtain escalated privileges and compromise the vulnerable system.

CVE-2023-24880 is another actively exploited vulnerability reported in Microsoft Windows SmartScreen that a remote attacker could employ to circumvent security restrictions on the targeted system. This vulnerability exists in Microsoft Windows SmartScreen as a result of a security bypass of Mark of the Web (MOTW) safeguards. An attacker could construct a malicious file that evades Mark of the Web (MOTW) safeguards, resulting in a limited loss of integrity and security feature availability. A remote attacker who successfully exploits this vulnerability could be able to circumvent security constraints on the targeted machine.

CVE-2023-23392 is an HTTP Protocol Stack vulnerability with a CVSS score of 9.8 that could allow an attacker to achieve remote code execution on vulnerable devices. It has an impact on Windows 11 and Windows Server 2022. CVE-2023-23415 is a severe Internet Control Message Protocol (ICMP) vulnerability that might allow Remote Code Execution Vulnerability. CVE-2023-21708 is a Remote Procedure Call Runtime Remote Code Execution Vulnerability in Windows 10 and 11 and Windows Servers. CVE-2023-23416 is a critical Remote Code Execution Vulnerability in Windows Cryptographic Services. According to Microsoft, these vulnerabilities are more likely to be exploited.

Organizations are recommended to consult Microsoft's Security Advisory, identify vulnerable instances, and apply the vendor-supplied fix as soon as feasible to thwart any exploitation efforts by threat actors.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft Patch Tuesday Mar 2023 - Fixes Two Exploited Zero-Days

Tracker ID: TN2343 **Date:** March 16, 2023 **Category:** Vulnerability **Industry:** All **Region**: All

Analysis

CVE ID	Severity	CVSS Score
CVE-2023-23397	Critical	9.8
CVE-2023-23392	Critical	9.8
CVE-2023-23415	Critical	9.8
CVE-2023-21708	Critical	9.8
CVE-2023-23416	High	8.4
CVE-2023-24880	Medium	5.4

Affected Products and Versions

- CVE-2023-23397 affects: Microsoft Outlook 2013, 2016 and 2019, Microsoft Office 2019, Microsoft 365 Apps for Enterprise and Microsoft Office LTSC 2021.
- CVE-2023-23392 affects: Windows 11 and Windows Server 2022
- CVE-2023-23415 and CVE-2023-21708 affects: Windows 10 and 11 versions and Windows Servers 2008, 2012, 2016, 2019, and 2022.
- CVE-2023-23416 affects : Windows 10 and 11 versions and Windows Servers 2012, 2016, 2019, and 2022..
- CVE-2023-24880 affects: Windows 10 and 11 versions and Windows Servers 2016, 2019and 2022.

Recommendations

- Administrators and organizations are encouraged to identify the vulnerable instances and implement the vendor-provided patch as soon as possible. Refer to the complete list of patched products here.

References

- Security Update Guide: Please apply filter for March, Microsoft, March 14th, 2023, External Link (msrc.microsoft.com).

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