BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

September 19, 2024

Microsoft Zero-Days and Related Vulnerabilities

SUMMARY

Microsoft's September 2024 Patch Tuesday release addresses 79 security vulnerabilities, including three actively exploited zero-day vulnerabilities and one publicly disclosed zero-day. The update also resolves 7 critical issues, involving either remote code execution (RCE) or privilege escalation.

The full report is here:

https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/Microsoft-Patch-Tuesday-September-2024.html

The number of bugs in each vulnerability category is listed below:

- 30 Elevation of Privilege Vulnerabilities
- 4 Security Feature Bypass Vulnerabilities
- 23 Remote Code Execution Vulnerabilities
- 11 Information Disclosure Vulnerabilities
- 8 Denial of Service Vulnerabilities
- 3 Spoofing Vulnerabilities

Zero-day Vulnerabilities fixed:

- Microsoft classifies a zero-day vulnerability as one that is either publicly disclosed or actively exploited while no official fix is available.

RISK SCORING

CVE-ID	CVSSv3 Score
CVE-2024-38014	7.8
CVE-2024-38217	5.4
CVE-2024-38226	7.3
CVE-2024-43491	9.8

VULNERABILITY DETAILS

The three actively exploited zero-day vulnerabilities patched in last Tuesday's updates are:

1. CVE-2024-38014 - Windows Installer Elevation of Privilege Vulnerability: This flaw allows attackers to gain SYSTEM privileges on Windows systems. Microsoft hasn't provided details on how it was used in attacks.
2. CVE-2024-38217 - Windows Mark of the Web (MOTW) Security Bypass Vulnerability: Publicly disclosed by Joe Desimone of Elastic Security, this flaw has likely been exploited since 2018. Desimone's report outlines 'LNK stomping,' a technique using specially crafted LNK files to

bypass Smart App Control and MOTW security warnings, allowing malicious files to be opened without alerts.

3. CVE-2024-38226 - Microsoft Publisher Security Feature Bypass Vulnerability: This vulnerability allows attackers to bypass Office macro policies that block untrusted or malicious files. Microsoft has not revealed the source of this discovery or how it was exploited.

PUBLICLY DISCLOSED ZERO-DAY

CVE-2024-43491 - Microsoft Windows Update Remote Code Execution Vulnerability

This flaw in the servicing stack, though labeled as remote code execution, actually rolls back fixes for older vulnerabilities in certain Windows components. Specifically, it affects Windows 10 version 1507 (released in July 2015) and certain supported versions like Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB. Microsoft clarified that while the flaw reintroduces previously exploited vulnerabilities, there is no evidence it was known or exploited externally before being discovered internally by Microsoft. According to Microsoft's advisory, systems that installed updates, including the March 2024 security update (KB5035858) through August 2024, were vulnerable to previously mitigated flaws being reintroduced in components such as Active Directory Lightweight Directory Services, Internet Explorer 11, and Windows Media Player.

RECOMMENDATIONS

- Apply security patches to all affected systems.
- CVE-2024-43491 is resolved by installing both the September 2024 Servicing Stack Update (KB5043936) and the September 2024 Windows security update (KB5043083) in-sequence.

REFERENCES

- https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2024-patch-tuesday-fixes-4-zero-days-79-flaws/
- https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/Microsoft-Patch-Tuesday-September-2024.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217
- https://nvd.nist.gov/vuln/detail/CVE-2024-38226
- https://nvd.nist.gov/vuln/detail/CVE-2024-43491
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-43461