TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

September 10, 2024

Executive Summary

The Microsoft Security Response Center (MSRC) reported 79 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 79 patched bugs, seven (7) were classified as critical severity. Four (4) actively exploited zero-day vulnerabilities, CVE-2024-38014, CVE-2024-38217, CVE-2024-38226 and CVE-2024-43491 were included in this Patch Tuesday release.

The number of bugs in each category is listed below:

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

Featured Critical Vulnerabilities

The seven (7) critical vulnerabilities/vulnerability listed in September's Patch Tuesday security update are listed below.

Windows Update	Microsoft Office SharePoint	Azure Stack	Azure Web Apps	Windows Network Address Translation (NAT)
CVE-2024-43491	CVE-2024-43464 CVE-2024-38018	CVE-2024-38220 CVE-2024-38216	CVE-2024-38194	CVE-2024-38119

Safeguards/Recommendations

Organizations should back up all systems, software, data, and device settings prior to performing updates and security patches. Users can regularly monitor the "Check for Updates" window in their Windows device settings to check if systems are up-to-date with the latest security patches.

For a full list of affected products, features, and roles, visit MSRC's September's 2024 Patch Tuesday release notes.

References

- https://msrc.microsoft.com/update-guide/releaseNote/2024-Sept
- https://msrc.microsoft.com/update-guide/vulnerability

Copyright © 2024. Security Risk Advisors Intl, LLC. All Rights Reserved