# TIGR Threat Bulletin

SecurityRisk ADVISORS

## Microsoft Patch Tuesday

August 08, 2023

### Executive Summary

The Microsoft Security Response Center (MSRC) reported 87 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 87 patched bugs, six (6) are classified as critical severity. Two (2) actively exploited zero-days were included in this Patch Tuesday release which is related to the vulnerability, CVE-2023-38180, and a defense in depth update ADV230003 which helps to mitigate CVE-2023-36884.

The number of bugs in each category is listed below:

- 18 Elevation of Privilege
- 3 Security Feature Bypass
- 23 Remote Code Execution (RCE)
- 10 Information Disclosure
- 8 Denial of Service (DoS)
- 12 Spoofing

### Featured Critical Vulnerabilities

The six (6) critical vulnerabilities listed in August's Patch Tuesday security updated are listed below.

| Microsoft Office Outlook | Microsoft Teams | Windows Message Queuing |
|---|---|---|
| CVE-2023-36895 | CVE-2023-29328<br>CVE-2023-29330 | CVE-2023-35385<br>CVE-2023-36911<br>CVE-2023-36910 |

### Safeguards/Recommendations

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

For a full list of affected products, features, and roles, visit MSRC's August 2023 Patch Tuesday release notes.

### References


- https://msrc.microsoft.com/update-guide/releaseNote/2023-Aug
- https://msrc.microsoft.com/update-guide/vulnerability
- https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2023-patch-tuesday-warns-of-2-zero-days-87-flaws/