

**Overall rating: Critical**



This is a technical bulletin intended for technical audiences.

### Summary

The Vulnerability and Risk Management (VRM) Team is aware Microsoft published security updates to address vulnerabilities in multiple products. Included were updates for the following products:

- Microsoft .NET – multiple versions
- Microsoft .NET Framework – multiple versions and platforms
- Microsoft Azure Kubernetes Service Confidential Containers – multiple versions
- Microsoft Defender for IoT – versions prior to 24.1.3
- Microsoft Office – multiple versions and platforms
- Microsoft SharePoint – multiple versions and platforms
- Microsoft SQL Server – multiple versions
- Microsoft Visual Studio – multiple versions and platforms
- Windows 10 – multiple platforms
- Windows 11 – multiple platforms
- Windows Server – multiple platforms

### Technical Details

○

<b>Exploitability Metrics</b> Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None
--

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

### Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify [VRM](#) with any questions or concerns you may have.

### References

- [CVE-2024-20665](#) [CVE-2024-20669](#) [CVE-2024-20670](#) [CVE-2024-20678](#) [CVE-2024-20685](#) [CVE-2024-20688](#) [CVE-2024-20689](#) [CVE-2024-20693](#) [CVE-2024-21322](#) [CVE-2024-21323](#) [CVE-2024-21324](#) [CVE-2024-21409](#) [CVE-2024-21424](#) [CVE-2024-21447](#) [CVE-2024-26158](#) [CVE-2024-26168](#) [CVE-2024-26171](#) [CVE-2024-26172](#) [CVE-2024-26175](#) [CVE-2024-26179](#) [CVE-2024-26180](#) [CVE-2024-26183](#) [CVE-2024-26189](#) [CVE-2024-26193](#) [CVE-2024-26194](#) [CVE-2024-26195](#) [CVE-2024-26200](#) [CVE-2024-26202](#) [CVE-2024-26205](#) [CVE-2024-26207](#) [CVE-2024-26208](#) [CVE-2024-26209](#) [CVE-2024-26210](#) [CVE-2024-26211](#) [CVE-2024-26212](#) [CVE-2024-26213](#) [CVE-2024-26214](#) [CVE-2024-26215](#) [CVE-2024-26216](#) [CVE-2024-26217](#) [CVE-2024-26218](#) [CVE-2024-26219](#) [CVE-2024-26220](#) [CVE-2024-26221](#) [CVE-2024-26222](#) [CVE-2024-26223](#) [CVE-2024-26224](#) [CVE-2024-26226](#) [CVE-2024-26227](#) [CVE-2024-26228](#) [CVE-2024-26229](#) [CVE-2024-26230](#) [CVE-2024-26231](#) [CVE-2024-26232](#) [CVE-2024-26233](#) [CVE-2024-26234](#) [CVE-2024-26235](#) [CVE-2024-26236](#) [CVE-2024-26237](#) [CVE-2024-26239](#) [CVE-2024-26240](#) [CVE-2024-26241](#) [CVE-2024-26242](#) [CVE-2024-26243](#) [CVE-2024-26244](#) [CVE-2024-26245](#) [CVE-2024-26248](#) [CVE-2024-26250](#) [CVE-2024-26251](#) [CVE-2024-26252](#) [CVE-2024-26253](#) [CVE-2024-26254](#) [CVE-2024-26255](#) [CVE-2024-26256](#) [CVE-2024-26257](#) [CVE-2024-28896](#) [CVE-2024-28897](#)

CVE-2024-28898 CVE-2024-28900 CVE-2024-28901 CVE-2024-28902 CVE-2024-28903 CVE-2024-28904 CVE-2024-28905 CVE-2024-28906 CVE-2024-28907 CVE-2024-28908 CVE-2024-28909 CVE-2024-28910 CVE-2024-28911 CVE-2024-28912 CVE-2024-28913 CVE-2024-28914 CVE-2024-28915 CVE-2024-28917 CVE-2024-28919 CVE-2024-28920 CVE-2024-28921 CVE-2024-28922 CVE-2024-28923 CVE-2024-28924 CVE-2024-28925 CVE-2024-28926 CVE-2024-28927 CVE-2024-28929 CVE-2024-28930 CVE-2024-28931 CVE-2024-28932 CVE-2024-28933 CVE-2024-28934 CVE-2024-28935 CVE-2024-28936 CVE-2024-28937 CVE-2024-28938 CVE-2024-28939 CVE-2024-28940 CVE-2024-28941 CVE-2024-28942 CVE-2024-28943 CVE-2024-28944 CVE-2024-28945 CVE-2024-29043 CVE-2024-29044 CVE-2024-29045 CVE-2024-29046 CVE-2024-29047 CVE-2024-29048 CVE-2024-29049 CVE-2024-29050 CVE-2024-29052 CVE-2024-29053 CVE-2024-29054 CVE-2024-29055 CVE-2024-29056 CVE-2024-29061 CVE-2024-29062 CVE-2024-29063 CVE-2024-29064 CVE-2024-29066 CVE-2024-29981 CVE-2024-29982 CVE-2024-29983 CVE-2024-29984 CVE-2024-29985 CVE-2024-29988 CVE-2024-29989 CVE-2024-29990 CVE-2024-29992 CVE-2024-29993

- [April 2024 Release Notes](#)
- [Security Update Guide](#)