September 11, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

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

- Azure Connected Machine Agent
- Azure CycleCloud – multiple versions and platforms
- Azure Health Bot
- Azure Network Watcher VM Extension for Windows
- Azure Stack Hub
- Azure Web Apps
- Microsoft 365 Apps for Enterprise – multiple platforms
- Microsoft AutoUpdate for Mac
- Microsoft Dynamics 365 (on-premises) – version 9.1
- Microsoft Dynamics 365 Business Central 2023 Release Wave 1
- Microsoft Excel 2016
- Microsoft Office – multiple versions and platforms
- Microsoft Outlook 2016 - multiple platforms
- Microsoft Project 2016 – multiple platforms
- Microsoft Publisher 2016
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SQL Server - multiple versions and platforms
- Microsoft Teams for iOS
- Microsoft Visio 2016 multiple platforms
- Microsoft Visual Studio 2022 – multiple versions
- .NET – version 8.0
- Power Automate for Desktop
- Remote Desktop client for Windows Desktop
- Windows 10 – multiple versions and platforms
- Windows 11 – multiple versions and platforms
- Windows Server – multiple versions and platforms

Microsoft has indicated that CVE-2024-38226, CVE-2024-43491, CVE-2024-38014 and CVE-2024-38217 have been exploited.

Technical Details

Windows TCP/IP	CVE-2024-21416	8.1
SQL Server	CVE-2024-26186	8.8
SQL Server	CVE-2024-26191	8.8
Windows Security Zone Mapping	CVE-2024-30073	7.8
SQL Server	CVE-2024-37335	8.8
SQL Server	CVE-2024-37337	7.1
SQL Server	CVE-2024-37338	8.8
SQL Server	CVE-2024-37339	8.8
SQL Server	CVE-2024-37340	8.8
SQL Server	CVE-2024-37341	8.8
SQL Server	CVE-2024-37342	7.1
SQL Server	CVE-2024-37965	8.8
SQL Server	CVE-2024-37966	7.1
SQL Server	CVE-2024-37980	8.8

Windows Installer	CVE-2024-38014	7.8
Microsoft Office SharePoint	CVE-2024-38018	8.8
Windows TCP/IP	CVE-2024-38045	8.1
Windows PowerShell	CVE-2024-38046	7.8
Windows Network Address Translation (NAT)	CVE-2024-38119	7.5
Azure Network Watcher	CVE-2024-38188	7.1
Azure Web Apps	CVE-2024-38194	8.4
Azure Stack	CVE-2024-38216	8.2
Windows Mark of the Web (MOTW)	CVE-2024-38217	5.4
Azure Stack	CVE-2024-38220	9
Dynamics Business Central	CVE-2024-38225	8.8
Microsoft Office Publisher	CVE-2024-38226	7.3
Microsoft Office SharePoint	CVE-2024-38227	7.2
Microsoft Office SharePoint	CVE-2024-38228	7.2
Windows Standards-Based Storage Management Service	CVE-2024-38230	6.5
Windows Remote Desktop Licensing Service	CVE-2024-38231	6.5
Windows Network Virtualization	CVE-2024-38232	7.5
Windows Network Virtualization	CVE-2024-38233	7.5
Windows Network Virtualization	CVE-2024-38234	6.5
Role: Windows Hyper-V	CVE-2024-38235	6.5
Windows DHCP Server	CVE-2024-38236	7.5
Microsoft Streaming Service	CVE-2024-38237	7.8
Microsoft Streaming Service	CVE-2024-38238	7.8
Windows Kerberos	CVE-2024-38239	7.2
Windows Remote Access Connection Manager	CVE-2024-38240	8.1
Microsoft Streaming Service	CVE-2024-38241	7.8
Microsoft Streaming Service	CVE-2024-38242	7.8
Microsoft Streaming Service	CVE-2024-38243	7.8
Microsoft Streaming Service	CVE-2024-38244	7.8
Microsoft Streaming Service	CVE-2024-38245	7.8
Windows Win32K - GRFX	CVE-2024-38246	7
Microsoft Graphics Component	CVE-2024-38247	7.8
Windows Storage	CVE-2024-38248	7
Microsoft Graphics Component	CVE-2024-38249	7.8
Microsoft Graphics Component	CVE-2024-38250	7.8
Windows Win32K - ICOMP	CVE-2024-38252	7.8
Windows Win32K - ICOMP	CVE-2024-38253	7.8
Windows Authentication Methods	CVE-2024-38254	5.5
Windows Kernel-Mode Drivers	CVE-2024-38256	5.5
Windows AllJoyn API	CVE-2024-38257	7.5
Windows Remote Desktop Licensing Service	CVE-2024-38258	6.5
Microsoft Management Console	CVE-2024-38259	8.8
Windows Remote Desktop Licensing Service	CVE-2024-38260	8.8
Windows Remote Desktop Licensing Service	CVE-2024-38263	7.5
Windows Remote Desktop Licensing Service	CVE-2024-43454	7.1
Windows Remote Desktop Licensing Service	CVE-2024-43455	8.8
Windows Setup and Deployment	CVE-2024-43457	7.8
Windows Network Virtualization	CVE-2024-43458	7.7
Windows MSHTML Platform	CVE-2024-43461	8.8
Microsoft Office Visio	CVE-2024-43463	7.8
Microsoft Office SharePoint	CVE-2024-43464	7.2
Microsoft Office Excel	CVE-2024-43465	7.8
Microsoft Office SharePoint	CVE-2024-43466	6.5
Windows Remote Desktop Licensing Service	CVE-2024-43467	7.5
Azure CycleCloud	CVE-2024-43469	8.8
Azure Network Watcher	CVE-2024-43470	7.3
SQL Server	CVE-2024-43474	7.6
Windows Admin Center	CVE-2024-43475	7.3
Microsoft Dynamics 365 (on-premises)	CVE-2024-43476	7.6

Power Automate	CVE-2024-43479	8.5
Microsoft Outlook for iOS	CVE-2024-43482	6.5
Windows Mark of the Web (MOTW)	CVE-2024-43487	6.5
Windows Update	CVE-2024-43491	9.8
Microsoft AutoUpdate (MAU)	CVE-2024-43492	7.8
Windows Libarchive	CVE-2024-43495	7.3

This vulnerability is rated as a **CRITICAL** risk. Software updates exist 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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- September 2024 Release Notes
- Security Update Guide