August 13, 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 Health Bot
- Azure Stack Hub
- Azure CycleCloud – multiple versions and platforms
- Microsoft 365 Apps for Enterprise – multiple platforms
- Microsoft Copilot Studio
- Microsoft Dynamics 365 (on-premises) – version 9.1
- Microsoft Office – multiple versions and platforms
- Microsoft Outlook 2016
- Microsoft Project 2016 – multiple platforms
- Microsoft Teams
- Microsoft Visual Studio – multiple versions and platforms
- .NET – version 8.0
- 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-2024-38189, CVE-2024-38107, CVE-2024-38106, CVE-2024-38213, CVE-2024-38193 and CVE-2024-38178 have been exploited.

Technical Details

Windows Secure Kernel Mode	CVE-2024-21302	6.7
Windows TCP/IP	CVE-2024-38063	9.8
Reliable Multicast Transport Driver (RMCAST)	CVE-2024-38140	9.8
Line Printer Daemon Service (LPD)	CVE-2024-38199	9.8
Azure Stack	CVE-2024-38108	9.3
Azure Health Bot	CVE-2024-38109	9.1
Windows Network Virtualization	CVE-2024-38159	9.1
Windows Network Virtualization	CVE-2024-38160	9.1
Windows IP Routing Management Snapin	CVE-2024-38114	8.8
Windows IP Routing Management Snapin	CVE-2024-38115	8.8
Windows IP Routing Management Snapin	CVE-2024-38116	8.8
Windows Routing and Remote Access Service (RRAS)	CVE-2024-38120	8.8
Windows Routing and Remote Access Service (RRAS)	CVE-2024-38121	8.8
Windows Routing and Remote Access Service (RRAS)	CVE-2024-38128	8.8
Windows Routing and Remote Access Service (RRAS)	CVE-2024-38130	8.8
Windows Clipboard Virtual Channel Extension	CVE-2024-38131	8.8
Microsoft Streaming Service	CVE-2024-38144	8.8
Windows Routing and Remote Access Service (RRAS)	CVE-2024-38154	8.8
Windows SmartScreen	CVE-2024-38180	8.8
Microsoft Office Project	CVE-2024-38189	8.8
Microsoft Copilot Studio	CVE-2024-38206	8.5
Microsoft Edge (Chromium-based)	CVE-2024-38218	8.4
Microsoft Dynamics	CVE-2024-38166	8.2

Microsoft Dynamics	CVE-2024-38211	8.2
Windows Kerberos	CVE-2024-29995	8.1
Microsoft Office	CVE-2024-38084	7.8
Azure Connected Machine Agent	CVE-2024-38098	7.8
Windows Power Dependency Coordinator	CVE-2024-38107	7.8
Windows NTFS	CVE-2024-38117	7.8
Microsoft Streaming Service	CVE-2024-38125	7.8
Windows Kernel	CVE-2024-38127	7.8
Windows Kernel	CVE-2024-38133	7.8
Microsoft Streaming Service	CVE-2024-38134	7.8
Windows NT OS Kernel	CVE-2024-38135	7.8
Windows Ancillary Function Driver for WinSock	CVE-2024-38141	7.8
Windows Secure Kernel Mode	CVE-2024-38142	7.8
Windows DWM Core Library	CVE-2024-38147	7.8
Windows DWM Core Library	CVE-2024-38150	7.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-38152	7.8
Windows Kernel	CVE-2024-38153	7.8
Azure Connected Machine Agent	CVE-2024-38162	7.8
Windows Update Stack	CVE-2024-38163	7.8
Microsoft Office Visio	CVE-2024-38169	7.8
Microsoft Office PowerPoint	CVE-2024-38171	7.8
Microsoft Office Excel	CVE-2024-38172	7.8
Windows App Installer	CVE-2024-38177	7.8
Windows Kernel-Mode Drivers	CVE-2024-38184	7.8
Windows Kernel-Mode Drivers	CVE-2024-38185	7.8
Windows Kernel-Mode Drivers	CVE-2024-38186	7.8
Windows Kernel-Mode Drivers	CVE-2024-38187	7.8
Windows Kernel-Mode Drivers	CVE-2024-38191	7.8
Windows Ancillary Function Driver for WinSock	CVE-2024-38193	7.8
Azure CycleCloud	CVE-2024-38195	7.8
Windows Common Log File System Driver	CVE-2024-38196	7.8
Windows Cloud Files Mini Filter Driver	CVE-2024-38215	7.8
Microsoft Windows DNS	CVE-2024-37968	7.5
Windows Network Address Translation (NAT)	CVE-2024-38126	7.5
Windows Network Address Translation (NAT)	CVE-2024-38132	7.5
Windows Deployment Services	CVE-2024-38138	7.5
Windows Layer-2 Bridge Network Driver	CVE-2024-38145	7.5
Windows Layer-2 Bridge Network Driver	CVE-2024-38146	7.5
Windows Transport Security Layer (TLS)	CVE-2024-38148	7.5
.NET and Visual Studio	CVE-2024-38168	7.5
Windows Scripting	CVE-2024-38178	7.5
Windows Print Spooler Components	CVE-2024-38198	7.5
Windows Update Stack	CVE-2024-38202	7.3
Microsoft Office Excel	CVE-2024-38170	7.1
Windows Kernel	CVE-2024-38106	7
Windows Resource Manager	CVE-2024-38136	7
Windows Resource Manager	CVE-2024-38137	7
Azure IoT SDK	CVE-2024-38157	7
Azure IoT SDK	CVE-2024-38158	7
Azure Stack	CVE-2024-38201	7
Windows Mobile Broadband	CVE-2024-38161	6.8
Windows Initial Machine Configuration	CVE-2024-38223	6.8
Microsoft Office Outlook	CVE-2024-38173	6.7
Windows Compressed Folder	CVE-2024-38165	6.5
.NET and Visual Studio	CVE-2024-38167	6.5
Microsoft Teams	CVE-2024-38197	6.5
Microsoft Office	CVE-2024-38200	6.5
Windows Mark of the Web (MOTW)	CVE-2024-38213	6.5
Windows Routing and Remote Access Service (RRAS)	CVE-2024-38214	6.5

Microsoft Edge (Chromium-based)	CVE-2024-38219	6.5
Microsoft Local Security Authority Server (lsasrv)	CVE-2024-38118	5.5
Microsoft Local Security Authority Server (lsasrv)	CVE-2024-38122	5.5
Windows Kernel	CVE-2024-38151	5.5
Windows Security Center	CVE-2024-38155	5.5
Microsoft Bluetooth Driver	CVE-2024-38123	4.4
Windows WLAN Auto Config Service	CVE-2024-38143	4.2
Microsoft Edge (Chromium-based)	CVE-2024-38222	

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

- August 2024 Release Notes
- Security Update Guide