July 9, 2024

Overall rating: Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Microsoft has published Security Updates to address vulnerabilities in multiple products.

Technical Details

On July 9, 2024, Microsoft published security advisories to address vulnerabilities in multiple products. Included were updates for the following products:

- Azure Network Watcher VM Extension for Windows
- Azure Kinect SDK
- Azure CycleCloud – multiple versions and platforms
- Azure DevOps Server 2022.1
- Microsoft 365 Apps for Enterprise – multiple platforms
- Microsoft .NET Framework – multiple versions and platforms
- Microsoft Defender for IoT
- Microsoft Dynamics 365 (on-premise) – version 9.1
- Microsoft OLE DB Driver for SQL Server – versions 18 and 19
- Microsoft Office – multiple versions and platforms
- Microsoft Outlook 2016
- Microsoft SQL Server – multiple versions and platforms
- Microsoft SharePoint Server – multiple versions and platforms
- Microsoft Visual Studio – multiple versions and platforms
- .NET – version 8.0
- Windows 10 – multiple versions and platforms
- Windows 11 – multiple versions and platforms
- Windows Server – multiple versions and platforms

Microsoft has indicated that CVE-2024-38112 and CVE-2024-38080 have been exploited.

SQL Server	CVE-2024-20701	8.8
SQL Server	CVE-2024-21303	8.8
SQL Server	CVE-2024-21308	8.8
SQL Server	CVE-2024-21317	8.8
SQL Server	CVE-2024-21331	8.8
SQL Server	CVE-2024-21332	8.8
SQL Server	CVE-2024-21333	8.8
SQL Server	CVE-2024-21335	8.8
SQL Server	CVE-2024-21373	8.8
SQL Server	CVE-2024-21398	8.8

SQL Server	CVE-2024-21414	8.8
SQL Server	CVE-2024-21415	8.8
Windows CoreMessaging	CVE-2024-21417	8.8
SQL Server	CVE-2024-21425	8.8
SQL Server	CVE-2024-21428	8.8
SQL Server	CVE-2024-21449	8.8
Windows Secure Boot	CVE-2024-26184	6.8
Windows Secure Boot	CVE-2024-28899	8.8
SQL Server	CVE-2024-28928	8.8
Windows MultiPoint Services	CVE-2024-30013	8.8
Microsoft Dynamics	CVE-2024-30061	7.3
Windows Remote Access Connection Manager	CVE-2024-30071	4.7
Windows Remote Access Connection Manager	CVE-2024-30079	7.8
Windows NTLM	CVE-2024-30081	7.1
Windows Cryptographic Services	CVE-2024-30098	7.5
.NET and Visual Studio	CVE-2024-30105	7.5
Microsoft Office SharePoint	CVE-2024-32987	7.5
SQL Server	CVE-2024-35256	8.8
Azure Network Watcher	CVE-2024-35261	7.8
.NET and Visual Studio	CVE-2024-35264	8.1
Azure DevOps	CVE-2024-35266	7.6
Azure DevOps	CVE-2024-35267	7.6
Windows iSCSI	CVE-2024-35270	5.3
SQL Server	CVE-2024-35271	8.8
SQL Server	CVE-2024-35272	8.8
SQL Server	CVE-2024-37318	8.8
SQL Server	CVE-2024-37319	8.8
SQL Server	CVE-2024-37320	8.8
SQL Server	CVE-2024-37321	8.8
SQL Server	CVE-2024-37322	8.8
SQL Server	CVE-2024-37323	8.8
SQL Server	CVE-2024-37324	8.8
SQL Server	CVE-2024-37326	8.8
SQL Server	CVE-2024-37327	8.8
SQL Server	CVE-2024-37328	8.8
SQL Server	CVE-2024-37329	8.8
SQL Server	CVE-2024-37330	8.8
SQL Server	CVE-2024-37331	8.8
SQL Server	CVE-2024-37332	8.8
SQL Server	CVE-2024-37333	8.8
SQL Server	CVE-2024-37334	8.8
SQL Server	CVE-2024-37336	8.8
Windows Secure Boot	CVE-2024-37969	8
Windows Secure Boot	CVE-2024-37970	8

Windows Secure Boot	CVE-2024-37971	8
Windows Secure Boot	CVE-2024-37972	8
Windows Secure Boot	CVE-2024-37973	8.4
Windows Secure Boot	CVE-2024-37974	8
Windows Secure Boot	CVE-2024-37975	8
Windows Secure Boot	CVE-2024-37977	8
Windows Secure Boot	CVE-2024-37978	8
Windows Secure Boot	CVE-2024-37981	8
Windows Secure Boot	CVE-2024-37984	8.4
Windows Secure Boot	CVE-2024-37986	8
Windows Secure Boot	CVE-2024-37987	8
Windows Secure Boot	CVE-2024-37988	8
Windows Secure Boot	CVE-2024-37989	8
Windows Secure Boot	CVE-2024-38010	8
Windows Secure Boot	CVE-2024-38011	8
Windows Server Backup	CVE-2024-38013	6.7
Windows Remote Desktop	CVE-2024-38015	7.5
Windows Message Queuing	CVE-2024-38017	5.5
Windows Performance Monitor	CVE-2024-38019	7.2
Microsoft Office Outlook	CVE-2024-38020	6.5
Microsoft Office	CVE-2024-38021	8.8
Windows Image Acquisition	CVE-2024-38022	7
Microsoft Office SharePoint	CVE-2024-38023	7.2
Microsoft Office SharePoint	CVE-2024-38024	7.2
Windows Performance Monitor	CVE-2024-38025	7.2
Line Printer Daemon Service (LPD)	CVE-2024-38027	6.5
Windows Performance Monitor	CVE-2024-38028	7.2
Windows Themes	CVE-2024-38030	6.5
Windows Online Certificate Status Protocol (OCSP)	CVE-2024-38031	7.5
XBox Crypto Graphic Services	CVE-2024-38032	7.1
Windows PowerShell	CVE-2024-38033	7.3
Windows Filtering	CVE-2024-38034	7.8
Windows Kernel	CVE-2024-38041	5.5
Windows PowerShell	CVE-2024-38043	7.8
Windows DHCP Server	CVE-2024-38044	7.2
Windows PowerShell	CVE-2024-38047	7.8
NDIS	CVE-2024-38048	6.5
Windows Distributed Transaction Coordinator	CVE-2024-38049	6.6
Windows Workstation Service	CVE-2024-38050	7.8
Microsoft Graphics Component	CVE-2024-38051	7.8
Microsoft Streaming Service	CVE-2024-38052	7.8
Windows Internet Connection Sharing (ICS)	CVE-2024-38053	8.8
Microsoft Streaming Service	CVE-2024-38054	7.8
Microsoft Windows Codecs Library	CVE-2024-38055	5.5

Microsoft Windows Codecs Library	CVE-2024-38056	5.5
Microsoft Streaming Service	CVE-2024-38057	7.8
Windows BitLocker	CVE-2024-38058	6.8
Windows Win32K - ICOMP	CVE-2024-38059	7.8
Microsoft Windows Codecs Library	CVE-2024-38060	8.8
Role: Active Directory Certificate Services; Active Directory Domain Services	CVE-2024-38061	7.5
Windows Kernel-Mode Drivers	CVE-2024-38062	7.8
Windows TCP/IP	CVE-2024-38064	7.5
Windows Secure Boot	CVE-2024-38065	6.8
Windows Win32K - GRFX	CVE-2024-38066	7.8
Windows Online Certificate Status Protocol (OCSP)	CVE-2024-38067	7.5
Windows Online Certificate Status Protocol (OCSP)	CVE-2024-38068	7.5
Windows Enroll Engine	CVE-2024-38069	7
Windows LockDown Policy (WLDP)	CVE-2024-38070	7.8
Windows Remote Desktop Licensing Service	CVE-2024-38071	7.5
Windows Remote Desktop Licensing Service	CVE-2024-38072	7.5
Windows Remote Desktop Licensing Service	CVE-2024-38073	7.5
Windows Remote Desktop Licensing Service	CVE-2024-38074	9.8
Active Directory Federation Services	CVE-2024-38075	7.4
Windows Remote Desktop	CVE-2024-38076	9.8
Windows Remote Desktop Licensing Service	CVE-2024-38077	9.8
XBox Crypto Graphic Services	CVE-2024-38078	7.5
Microsoft Graphics Component	CVE-2024-38079	7.8
Role: Windows Hyper-V	CVE-2024-38080	7.8
.NET and Visual Studio	CVE-2024-38081	7.3
Windows Win32 Kernel Subsystem	CVE-2024-38085	7.8
Azure Kinect SDK	CVE-2024-38086	6.4
SQL Server	CVE-2024-38087	8.8
SQL Server	CVE-2024-38088	8.8
Microsoft Defender for IoT	CVE-2024-38089	9.1
Microsoft WS-Discovery	CVE-2024-38091	7.5
Azure CycleCloud	CVE-2024-38092	8.8
Microsoft Office SharePoint	CVE-2024-38094	7.2
.NET and Visual Studio	CVE-2024-38095	7.5
Windows Remote Desktop Licensing Service	CVE-2024-38099	5.9
Windows COM Session	CVE-2024-38100	7.8
Windows Internet Connection Sharing (ICS)	CVE-2024-38101	6.5
Windows Internet Connection Sharing (ICS)	CVE-2024-38102	6.5
Windows Fax and Scan Service	CVE-2024-38104	8.8
Windows Internet Connection Sharing (ICS)	CVE-2024-38105	6.5
Windows MSHTML Platform	CVE-2024-38112	7.5

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- July 2024 Release Notes
- Security Update Guide