February 13, 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 January 9, 2024, Microsoft published security updates to address vulnerabilities in multiple products. Included were critical updates for the following products:

- Microsoft 365 Apps for Enterprise – multiple platforms
- Microsoft Dynamics 365 Business Central – multiple versions and platforms
- Microsoft Exchange Server 2016 and 2019 – multiple platforms
- Microsoft Office 2016, 2019 and LTSC – multiple platforms
- Windows 10 – multiple platforms
- Windows 11 – multiple platforms
- Windows Server – multiple platforms

Microsoft has indicated that CVE-2024-21412 and CVE-2024-21351 have been exploited.
Updated products:

Azure DevOps	CVE-2024-20667	7.5
Microsoft Office	CVE-2024-20673	7.8
Azure Stack	CVE-2024-20679	6.5
Windows Hyper-V	CVE-2024-20684	6.5
Skype for Business	CVE-2024-20695	5.7
Trusted Compute Base	CVE-2024-21304	4.1
Microsoft Defender for Endpoint	CVE-2024-21315	7.8
Microsoft Dynamics	CVE-2024-21327	7.6
Microsoft Dynamics	CVE-2024-21328	7.6
Azure Connected Machine Agent	CVE-2024-21329	7.3
Windows Kernel	CVE-2024-21338	7.8
Windows USB Serial Driver	CVE-2024-21339	6.4
Windows Kernel	CVE-2024-21340	4.6
Windows Kernel	CVE-2024-21341	6.8
Role: DNS Server	CVE-2024-21342	7.5
Windows Internet Connection Sharing (ICS)	CVE-2024-21343	5.9
Windows Internet Connection Sharing (ICS)	CVE-2024-21344	5.9
Windows Kernel	CVE-2024-21345	8.8

Windows Win32K - ICOMP	CVE-2024-21346	7.8
SQL Server	CVE-2024-21347	7.5
Windows Internet Connection Sharing (ICS)	CVE-2024-21348	7.5
Microsoft ActiveX	CVE-2024-21349	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21350	8.8
Windows SmartScreen	CVE-2024-21351	7.6
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21352	8.8
Microsoft WDAC ODBC Driver	CVE-2024-21353	8.8
Windows Message Queuing	CVE-2024-21354	7.8
Windows Message Queuing	CVE-2024-21355	7
Windows LDAP - Lightweight Directory Access Protocol	CVE-2024-21356	6.5
Windows Internet Connection Sharing (ICS)	CVE-2024-21357	7.5
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21358	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21359	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21360	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21361	8.8
Windows Kernel	CVE-2024-21362	5.5
Windows Message Queuing	CVE-2024-21363	7.8
Azure Site Recovery	CVE-2024-21364	9.3
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21365	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21366	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21367	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21368	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21369	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21370	8.8
Windows Kernel	CVE-2024-21371	7
Windows OLE	CVE-2024-21372	8.8
Microsoft Teams for Android	CVE-2024-21374	5
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21375	8.8
Microsoft Azure Kubernetes Service	CVE-2024-21376	9
Microsoft Windows DNS	CVE-2024-21377	7.1
Microsoft Office Outlook	CVE-2024-21378	8
Microsoft Office Word	CVE-2024-21379	7.8
Microsoft Dynamics	CVE-2024-21380	8
Azure Active Directory	CVE-2024-21381	6.8
Microsoft Office OneNote	CVE-2024-21384	7.8
.NET	CVE-2024-21386	7.5
Microsoft Dynamics	CVE-2024-21389	7.6
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21391	8.8
Microsoft Dynamics	CVE-2024-21393	7.6
Microsoft Dynamics	CVE-2024-21394	7.6
Microsoft Dynamics	CVE-2024-21395	8.2
Microsoft Dynamics	CVE-2024-21396	7.6
Azure File Sync	CVE-2024-21397	5.3

Microsoft Edge (Chromium-based)	CVE-2024-21399	8.3
Azure Active Directory	CVE-2024-21401	9.8
Microsoft Office Outlook	CVE-2024-21402	7.1
Microsoft Azure Kubernetes Service	CVE-2024-21403	9
.NET	CVE-2024-21404	7.5
Windows Message Queuing	CVE-2024-21405	7
Microsoft Windows	CVE-2024-21406	7.5
Microsoft Exchange Server	CVE-2024-21410	9.8
Internet Shortcut Files	CVE-2024-21412	6.8
Microsoft Office	CVE-2024-21413	9.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21420	8.8

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

- February 2024 Release Notes
- Security Update Guide