Overall rating: High

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

Updated products:

Tag	CVE	Base Score
Azure DevOps	CVE-2023-21565	7.1
Azure DevOps	CVE-2023-21569	5.5
.NET and Visual Studio	CVE-2023-24895	7.8
Microsoft Dynamics	CVE-2023-24896	5.4
.NET and Visual Studio	CVE-2023-24897	7.8
.NET and Visual Studio	CVE-2023-24936	8.1
Windows CryptoAPI	CVE-2023-24937	6.5
Windows CryptoAPI	CVE-2023-24938	6.5
Microsoft Exchange Server	CVE-2023-28310	8
.NET Framework	CVE-2023-29326	7.8
.NET Core	CVE-2023-29331	7.5
NuGet Client	CVE-2023-29337	7.1
Microsoft Edge (Chromium-based)	CVE-2023-29345	6.1
Windows NTFS	CVE-2023-29346	7.8
Windows Group Policy	CVE-2023-29351	8.1
Remote Desktop Client	CVE-2023-29352	6.5
SysInternals	CVE-2023-29353	5.5
Windows DHCP Server	CVE-2023-29355	5.3
Microsoft Office SharePoint	CVE-2023-29357	9.8
Windows GDI	CVE-2023-29358	7.8
Windows Win32K	CVE-2023-29359	7.8
Windows TPM Device Driver	CVE-2023-29360	7.8
Windows Cloud Files Mini Filter Driver	CVE-2023-29361	7
Remote Desktop Client	CVE-2023-29362	8.8
Windows PGM	CVE-2023-29363	9.8
Windows Authentication Methods	CVE-2023-29364	7
Microsoft Windows Codecs Library	CVE-2023-29365	7.8
Windows Geolocation Service	CVE-2023-29366	7.8
Windows OLE	CVE-2023-29367	7.8

Windows Filtering	CVE-2023-29368	7
Windows Remote Procedure Call Runtime	CVE-2023-29369	6.5
Microsoft Windows Codecs Library	CVE-2023-29370	7.8
Windows Win32K	CVE-2023-29371	7.8
Microsoft WDAC OLE DB provider for SQL	CVE-2023-29372	8.8
Windows ODBC Driver	CVE-2023-29373	8.8
Windows Resilient File System (ReFS)	CVE-2023-32008	7.8
Windows Collaborative Translation Framework	CVE-2023-32009	8.8
Windows Bus Filter Driver	CVE-2023-32010	7
Windows iSCSI	CVE-2023-32011	7.5
Windows Container Manager Service	CVE-2023-32012	6.3
Windows Hyper-V	CVE-2023-32013	6.5
Windows PGM	CVE-2023-32014	9.8
Windows PGM	CVE-2023-32015	9.8
Windows Installer	CVE-2023-32016	5.5
Microsoft Printer Drivers	CVE-2023-32017	7.8
Windows Hello	CVE-2023-32018	7.8
Windows Kernel	CVE-2023-32019	4.7
Role: DNS Server	CVE-2023-32020	3.7
Windows SMB	CVE-2023-32021	7.1
Windows Server Service	CVE-2023-32022	7.6
Microsoft Power Apps	CVE-2023-32024	3
Microsoft Office Excel	CVE-2023-32029	7.8
.NET and Visual Studio	CVE-2023-32030	7.5
Microsoft Exchange Server	CVE-2023-32031	8.8
.NET and Visual Studio	CVE-2023-32032	6.5
.NET and Visual Studio	CVE-2023-33126	7.3
.NET and Visual Studio	CVE-2023-33127	8.1
.NET and Visual Studio	CVE-2023-33128	7.3
Microsoft Office SharePoint	CVE-2023-33129	6.5
Microsoft Office SharePoint	CVE-2023-33130	7.3
Microsoft Office Outlook	CVE-2023-33131	8.8
Microsoft Office SharePoint	CVE-2023-33132	6.3
Microsoft Office Excel	CVE-2023-33133	7.8
.NET and Visual Studio	CVE-2023-33135	7.3
Microsoft Office Excel	CVE-2023-33137	7.8
Visual Studio	CVE-2023-33139	5.5
Microsoft Office OneNote	CVE-2023-33140	6.5
ASP .NET	CVE-2023-33141	7.5
Microsoft Office SharePoint	CVE-2023-33142	6.5
Microsoft Edge (Chromium-based)	CVE-2023-33143	7.5
Visual Studio Code	CVE-2023-33144	5
Microsoft Edge (Chromium-based)	CVE-2023-33145	6.5

Microsoft Office	CVE-2023-33146	7.8

These vulnerabilities are rated as an overall **High** 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

- June 2023 Release Notes
- Security Update Guide