May 14, 2024

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 published security advisories to address vulnerabilities in multiple products. Included were updates for the following products:

- Dynamics 365 Customer Insights
- Microsoft 365 Apps for Enterprise
- Microsoft Excel 2016
- Microsoft .NET 7.0 and 8.0
- Microsoft Office – multiple versions and platforms
- Microsoft SharePoint – multiple versions and platforms
- Microsoft SharePoint Server – multiple versions and platforms
- Microsoft Visual Studio – multiple versions and platforms
- Office Online Server
- Windows 10 – multiple platforms and versions
- Windows 11 – multiple platforms and versions
- Windows Server – multiple platforms

Microsoft has indicated that CVE-2024-30040 and CVE-2024-30051 have been exploited.

Technical Details

Windows Task Scheduler	CVE-2024-26238	7.8
Microsoft Windows SCSI Class System File	CVE-2024-29994	7.8
Windows Common Log File System Driver	CVE-2024-29996	7.8
Windows Mobile Broadband	CVE-2024-29997	6.8
Windows Mobile Broadband	CVE-2024-29998	6.8
Windows Mobile Broadband	CVE-2024-29999	6.8
Windows Mobile Broadband	CVE-2024-30000	6.8
Windows Mobile Broadband	CVE-2024-30001	6.8
Windows Mobile Broadband	CVE-2024-30002	6.8
Windows Mobile Broadband	CVE-2024-30003	6.8
Windows Mobile Broadband	CVE-2024-30004	6.8
Windows Mobile Broadband	CVE-2024-30005	6.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-30006	8.8
Microsoft Brokering File System	CVE-2024-30007	8.8

Windows DWM Core Library	CVE-2024-30008	5.5
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30009	8.8
Windows Hyper-V	CVE-2024-30010	8.8
Windows Hyper-V	CVE-2024-30011	6.5
Windows Mobile Broadband	CVE-2024-30012	6.8
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30014	7.5
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30015	7.5
Windows Cryptographic Services	CVE-2024-30016	5.5
Windows Hyper-V	CVE-2024-30017	8.8
Windows Kernel	CVE-2024-30018	7.8
Windows DHCP Server	CVE-2024-30019	6.5
Windows Cryptographic Services	CVE-2024-30020	8.1
Windows Mobile Broadband	CVE-2024-30021	6.8
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30022	7.5
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30023	7.5
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30024	7.5
Windows Common Log File System Driver	CVE-2024-30025	7.8
Windows NTFS	CVE-2024-30027	7.8
Windows Win32K - ICOMP	CVE-2024-30028	7.8
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30029	7.5
Windows Win32K - GRFX	CVE-2024-30030	7.8
Windows CNG Key Isolation Service	CVE-2024-30031	7.8
Windows DWM Core Library	CVE-2024-30032	7.8
Microsoft Windows Search Component	CVE-2024-30033	7
Windows Cloud Files Mini Filter Driver	CVE-2024-30034	5.5
Windows DWM Core Library	CVE-2024-30035	7.8
Windows Deployment Services	CVE-2024-30036	6.5
Windows Common Log File System Driver	CVE-2024-30037	7.5
Windows Win32K - ICOMP	CVE-2024-30038	7.8
Windows Remote Access Connection Manager	CVE-2024-30039	5.5
Windows MSHTML Platform	CVE-2024-30040	8.8
Microsoft Bing	CVE-2024-30041	5.4
Microsoft Office Excel	CVE-2024-30042	7.8
Microsoft Office SharePoint	CVE-2024-30043	6.5
Microsoft Office SharePoint	CVE-2024-30044	8.8
.NET and Visual Studio	CVE-2024-30045	6.3
Visual Studio	CVE-2024-30046	5.9

Microsoft Dynamics 365 Customer Insights	CVE-2024-30047	7.6
Microsoft Dynamics 365 Customer Insights	CVE-2024-30048	7.6
Windows Win32K - ICOMP	CVE-2024-30049	7.8
Windows Mark of the Web (MOTW)	CVE-2024-30050	5.4
Windows DWM Core Library	CVE-2024-30051	7.8
Azure Migrate	CVE-2024-30053	6.5
Power BI	CVE-2024-30054	6.5
Microsoft Edge (Chromium-based)	CVE-2024-30055	5.4
Microsoft Intune	CVE-2024-30059	6.1

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

- May 2024 Release Notes
- Security Update Guide