June 12, 2024

Overall Rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made of Microsoft's June Security Advisory impacting multiple Microsoft products with 51 published vulnerabilities from CRITICAL to MEDIUM risks.

Technical Details

The CVE links will provide additional details of the vulnerability, the products impacted, attack vector and potential mitigation steps. Although CVE-2024-30080 has a CRITICAL risk, the temporal score is an 8.5 HIGH assessment, as such the overall risk for the June Microsoft Security Advisory is **HIGH**.

Application	CVE	Base Score	Risk
Windows Server Service	CVE-2024-30080	9.8	**Critical**
Windows Server Service	CVE-2024-30062	7.8	**High**
Windows Kernel	CVE-2024-30064	8.8	**High**
Windows Kernel	CVE-2024-30068	8.8	**High**
Windows DHCP Server	CVE-2024-30070	7.5	**High**
Windows Event Logging Service	CVE-2024-30072	7.8	**High**
Windows Link Layer Topology Discovery Protocol	CVE-2024-30074	8.0	**High**
Windows Link Layer Topology Discovery Protocol	CVE-2024-30075	8.0	**High**
Microsoft WDAC OLE DB provider for SQL	CVE-2024-30077	8.0	**High**
Windows Wi-Fi Driver	CVE-2024-30078	8.8	**High**
Windows Win32K - GRFX	CVE-2024-30082	7.8	**High**
Windows Standards-Based Storage Management Service	CVE-2024-30083	7.5	**High**
Windows Kernel-Mode Drivers	CVE-2024-30084	7.0	**High**
Windows Cloud Files Mini Filter Driver	CVE-2024-30085	7.8	**High**
Windows Win32 Kernel Subsystem	CVE-2024-30086	7.8	**High**
Windows Win32K - GRFX	CVE-2024-30087	7.8	**High**
Windows NT OS Kernel	CVE-2024-30088	7.0	**High**
Microsoft Streaming Service	CVE-2024-30089	7.8	**High**
Microsoft Streaming Service	CVE-2024-30090	7.0	**High**
Windows Win32K - GRFX	CVE-2024-30091	7.8	**High**
Windows Storage	CVE-2024-30093	7.3	**High**
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30094	7.8	**High**
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30095	7.8	**High**
Microsoft Windows Speech	CVE-2024-30097	8.8	**High**
Windows NT OS Kernel	CVE-2024-30099	7.0	**High**
Microsoft Office SharePoint	CVE-2024-30100	7.8	**High**
Microsoft Office	CVE-2024-30101	7.5	**High**
Microsoft Office Word	CVE-2024-30102	7.3	**High**
Microsoft Office Outlook	CVE-2024-30103	8.8	**High**
Microsoft Office	CVE-2024-30104	7.8	**High**
Dynamics Business Central	CVE-2024-35248	7.3	**High**

Dynamics Business Central	CVE-2024-35249	8.8	**High**
Windows Kernel-Mode Drivers	CVE-2024-35250	7.8	**High**
Azure Storage Library	CVE-2024-35252	7.5	**High**
Azure Monitor	CVE-2024-35254	7.1	**High**
Windows Perception Service	CVE-2024-35265	7.0	**High**
Azure Data Science Virtual Machines	CVE-2024-37325	8.1	**High**
Visual Studio	CVE-2024-29060	6.7	**Medium**
Visual Studio	CVE-2024-30052	4.7	**Medium**
Windows Distributed File System (DFS)	CVE-2024-30063	6.7	**Medium**
Windows Themes	CVE-2024-30065	5.5	**Medium**
Winlogon	CVE-2024-30066	5.5	**Medium**
Winlogon	CVE-2024-30067	5.5	**Medium**
Windows Remote Access Connection Manager	CVE-2024-30069	4.7	**Medium**
Windows Container Manager Service	CVE-2024-30076	6.8	**Medium**
Windows Cryptographic Services	CVE-2024-30096	5.5	**Medium**
Azure File Sync	CVE-2024-35253	4.4	**Medium**
Azure SDK	CVE-2024-35255	5.5	**Medium**
Microsoft Dynamics	CVE-2024-35263	5.7	**Medium**

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

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 atVulnerabilityandRiskManagement@gov.bc.ca.

References

- June 2024 Security Updates
- VRM Vulnerability Reports