January 9, 2024

Overall rating: Critical

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:

- Windows 10 – multiple platforms
- Windows 11 – multiple platforms
- Windows Server – multiple platforms

Updated products:

SQL Server	CVE-2024-0056	8.7
.NET and Visual Studio	CVE-2024-0057	9.1
Windows Scripting	CVE-2024-20652	7.5
Windows Common Log File System Driver	CVE-2024-20653	7.8
Windows ODBC Driver	CVE-2024-20654	8
Windows Online Certificate Status Protocol (OCSP) SnapIn	CVE-2024-20655	6.6
Visual Studio	CVE-2024-20656	7.8
Windows Group Policy	CVE-2024-20657	7
Microsoft Virtual Hard Drive	CVE-2024-20658	7.8
Windows Message Queuing	CVE-2024-20660	6.5
Windows Message Queuing	CVE-2024-20661	7.5
Windows Online Certificate Status Protocol (OCSP) SnapIn	CVE-2024-20662	4.9
Windows Message Queuing	CVE-2024-20663	6.5
Windows Message Queuing	CVE-2024-20664	6.5
Windows BitLocker	CVE-2024-20666	6.6
.NET Core & Visual Studio	CVE-2024-20672	7.5
Windows Authentication Methods	CVE-2024-20674	9
Azure Storage Mover	CVE-2024-20676	8
Microsoft Office	CVE-2024-20677	7.8
Windows Message Queuing	CVE-2024-20680	6.5
Windows Subsystem for Linux	CVE-2024-20681	7.8
Windows Cryptographic Services	CVE-2024-20682	7.8

Windows Win32K	CVE-2024-20683	7.8
Windows Win32 Kernel Subsystem	CVE-2024-20686	7.8
Windows AllJoyn API	CVE-2024-20687	7.5
Windows Nearby Sharing	CVE-2024-20690	6.5
Windows Themes	CVE-2024-20691	4.7
Windows Local Security Authority Subsystem Service (LSASS)	CVE-2024-20692	5.7
Windows Collaborative Translation Framework	CVE-2024-20694	5.5
Windows Libarchive	CVE-2024-20696	7.3
Windows Libarchive	CVE-2024-20697	7.3
Windows Kernel	CVE-2024-20698	7.8
Windows Hyper-V	CVE-2024-20699	5.5
Windows Hyper-V	CVE-2024-20700	7.5
Unified Extensible Firmware Interface	CVE-2024-21305	4.4
Microsoft Bluetooth Driver	CVE-2024-21306	5.7
Remote Desktop Client	CVE-2024-21307	7.5
Windows Kernel-Mode Drivers	CVE-2024-21309	7.8
Windows Cloud Files Mini Filter Driver	CVE-2024-21310	7.8
Windows Cryptographic Services	CVE-2024-21311	5.5
.NET Framework	CVE-2024-21312	7.5
Windows TCP/IP	CVE-2024-21313	5.3
Windows Message Queuing	CVE-2024-21314	6.5
Windows Server Key Distribution Service	CVE-2024-21316	6.1
Microsoft Office SharePoint	CVE-2024-21318	8.8
Microsoft Identity Services	CVE-2024-21319	6.8
Windows Themes	CVE-2024-21320	6.5
Microsoft Devices	CVE-2024-21325	7.8
SQL Server	CVE-2024-0056	8.7
.NET and Visual Studio	CVE-2024-0057	9.1
Windows Scripting	CVE-2024-20652	7.5
Windows Common Log File System Driver	CVE-2024-20653	7.8
Windows ODBC Driver	CVE-2024-20654	8
Windows Online Certificate Status Protocol (OCSP) SnapIn	CVE-2024-20655	6.6
Visual Studio	CVE-2024-20656	7.8
Windows Group Policy	CVE-2024-20657	7
Microsoft Virtual Hard Drive	CVE-2024-20658	7.8
Windows Message Queuing	CVE-2024-20660	6.5
Windows Message Queuing	CVE-2024-20661	7.5
Windows Online Certificate Status Protocol (OCSP) SnapIn	CVE-2024-20662	4.9
Windows Message Queuing	CVE-2024-20663	6.5
Windows Message Queuing	CVE-2024-20664	6.5
Windows BitLocker	CVE-2024-20666	6.6
.NET Core & Visual Studio	CVE-2024-20672	7.5
Windows Authentication Methods	CVE-2024-20674	9
Azure Storage Mover	CVE-2024-20676	8

Microsoft Office	CVE-2024-20677	7.8
Windows Message Queuing	CVE-2024-20680	6.5
Windows Subsystem for Linux	CVE-2024-20681	7.8
Windows Cryptographic Services	CVE-2024-20682	7.8
Windows Win32K	CVE-2024-20683	7.8
Windows Win32 Kernel Subsystem	CVE-2024-20686	7.8
Windows AllJoyn API	CVE-2024-20687	7.5
Windows Nearby Sharing	CVE-2024-20690	6.5
Windows Themes	CVE-2024-20691	4.7
Windows Local Security Authority Subsystem Service (LSASS)	CVE-2024-20692	5.7
Windows Collaborative Translation Framework	CVE-2024-20694	5.5
Windows Libarchive	CVE-2024-20696	7.3
Windows Libarchive	CVE-2024-20697	7.3
Windows Kernel	CVE-2024-20698	7.8
Windows Hyper-V	CVE-2024-20699	5.5
Windows Hyper-V	CVE-2024-20700	7.5
Unified Extensible Firmware Interface	CVE-2024-21305	4.4
Microsoft Bluetooth Driver	CVE-2024-21306	5.7
Remote Desktop Client	CVE-2024-21307	7.5
Windows Kernel-Mode Drivers	CVE-2024-21309	7.8
Windows Cloud Files Mini Filter Driver	CVE-2024-21310	7.8
Windows Cryptographic Services	CVE-2024-21311	5.5
.NET Framework	CVE-2024-21312	7.5
Windows TCP/IP	CVE-2024-21313	5.3
Windows Message Queuing	CVE-2024-21314	6.5
Windows Server Key Distribution Service	CVE-2024-21316	6.1
Microsoft Office SharePoint	CVE-2024-21318	8.8
Microsoft Identity Services	CVE-2024-21319	6.8
Windows Themes	CVE-2024-21320	6.5
Microsoft Devices	CVE-2024-21325	7.8

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

- January 2024 Release Notes
- Security Update Guide