October 11, 2023

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 October 10, 2023, 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

Microsoft has indicated that CVE-2023-44487, CVE-2023-36563 and CVE-2023-41763 have been exploited.
Updated products:

Windows RDP	CVE-2023-29348	6.5
Windows Message Queuing	CVE-2023-35349	9.8
Azure SDK	CVE-2023-36414	8.8
Azure SDK	CVE-2023-36415	8.8
Microsoft Dynamics	CVE-2023-36416	6.1
SQL Server	CVE-2023-36417	7.8
Azure Real Time Operating System	CVE-2023-36418	7.8
Azure	CVE-2023-36419	8.8
SQL Server	CVE-2023-36420	7.3
Microsoft Dynamics	CVE-2023-36429	6.5
Windows Message Queuing	CVE-2023-36431	7.5
Microsoft Dynamics	CVE-2023-36433	6.5
Windows IIS	CVE-2023-36434	9.8
Microsoft QUIC	CVE-2023-36435	7.5
Windows HTML Platform	CVE-2023-36436	7.8
Windows TCP/IP	CVE-2023-36438	7.5
Windows HTML Platform	CVE-2023-36557	7.8
Azure DevOps	CVE-2023-36561	7.3
Microsoft WordPad	CVE-2023-36563	6.5
Microsoft Windows Search Component	CVE-2023-36564	6.5

Microsoft Office	CVE-2023-36565	7.0
Microsoft Common Data Model SDK	CVE-2023-36566	6.5
Windows Deployment Services	CVE-2023-36567	7.5
Microsoft Office	CVE-2023-36568	7.0
Microsoft Office	CVE-2023-36569	8.4
Windows Message Queuing	CVE-2023-36570	7.3
Windows Message Queuing	CVE-2023-36571	7.3
Windows Message Queuing	CVE-2023-36572	7.3
Windows Message Queuing	CVE-2023-36573	7.3
Windows Message Queuing	CVE-2023-36574	7.3
Windows Message Queuing	CVE-2023-36575	7.3
Windows Kernel	CVE-2023-36576	5.5
Microsoft WDAC OLE DB provider for SQL	CVE-2023-36577	8.8
Windows Message Queuing	CVE-2023-36578	7.3
Windows Message Queuing	CVE-2023-36579	7.5
Windows Message Queuing	CVE-2023-36581	7.5
Windows Message Queuing	CVE-2023-36582	7.3
Windows Message Queuing	CVE-2023-36583	7.3
Windows Mark of the Web (MOTW)	CVE-2023-36584	5.4
Windows Active Template Library	CVE-2023-36585	7.5
Windows Message Queuing	CVE-2023-36589	7.3
Windows Message Queuing	CVE-2023-36590	7.3
Windows Message Queuing	CVE-2023-36591	7.3
Windows Message Queuing	CVE-2023-36592	7.3
Windows Message Queuing	CVE-2023-36593	7.8
Microsoft Graphics Component	CVE-2023-36594	7.8
Windows Remote Procedure Call	CVE-2023-36596	6.5
SQL Server	CVE-2023-36598	7.8
Windows TCP/IP	CVE-2023-36602	7.5
Windows TCP/IP	CVE-2023-36603	7.5
Windows Named Pipe File System	CVE-2023-36605	7.4
Windows Message Queuing	CVE-2023-36606	7.5
Windows Message Queuing	CVE-2023-36697	6.8
Windows Kernel	CVE-2023-36698	3.6
Windows Resilient File System (ReFS)	CVE-2023-36701	7.8
Windows Microsoft DirectMusic	CVE-2023-36702	7.8
Windows DHCP Server	CVE-2023-36703	7.5
Windows Setup Files Cleanup	CVE-2023-36704	7.8
Windows Deployment Services	CVE-2023-36706	6.5
Windows Deployment Services	CVE-2023-36707	6.5
Windows AllJoyn API	CVE-2023-36709	7.5
Microsoft Windows Media Foundation	CVE-2023-36710	7.8
Windows Runtime C++ Template Library	CVE-2023-36711	7.8
Windows Kernel	CVE-2023-36712	7.8

Windows Common Log File System Driver	CVE-2023-36713	5.5
Windows TPM	CVE-2023-36717	6.5
Windows Virtual Trusted Platform Module	CVE-2023-36718	7.8
Windows Mixed Reality Developer Tools	CVE-2023-36720	7.5
Windows Error Reporting	CVE-2023-36721	7.0
Active Directory Domain Services	CVE-2023-36722	4.4
Windows Container Manager Service	CVE-2023-36723	7.8
Windows Power Management Service	CVE-2023-36724	5.5
Windows NT OS Kernel	CVE-2023-36725	7.8
Windows IKE Extension	CVE-2023-36726	7.8
SQL Server	CVE-2023-36728	5.5
Windows Named Pipe File System	CVE-2023-36729	7.8
SQL Server	CVE-2023-36730	7.8
Windows Win32K	CVE-2023-36731	7.8
Windows Win32K	CVE-2023-36732	7.8
Azure	CVE-2023-36737	7.8
Windows Win32K	CVE-2023-36743	7.8
Windows Win32K	CVE-2023-36776	7.0
Microsoft Exchange Server	CVE-2023-36778	8.0
Skype for Business	CVE-2023-36780	7.2
SQL Server	CVE-2023-36785	7.8
Skype for Business	CVE-2023-36786	7.2
Skype for Business	CVE-2023-36789	7.2
Windows RDP	CVE-2023-36790	7.8
Windows Client/Server Runtime Subsystem	CVE-2023-36902	7.0
Microsoft Graphics Component	CVE-2023-38159	7.0
Windows Layer 2 Tunneling Protocol	CVE-2023-38166	8.1
Microsoft QUIC	CVE-2023-38171	7.5
Skype for Business	CVE-2023-41763	5.3
Windows Layer 2 Tunneling Protocol	CVE-2023-41765	8.1
Client Server Run-time Subsystem (CSRSS)	CVE-2023-41766	7.8
Windows Layer 2 Tunneling Protocol	CVE-2023-41767	8.1
Windows Layer 2 Tunneling Protocol	CVE-2023-41768	8.1
Windows Layer 2 Tunneling Protocol	CVE-2023-41769	8.1
Windows Layer 2 Tunneling Protocol	CVE-2023-41770	8.1
Windows Layer 2 Tunneling Protocol	CVE-2023-41771	8.1
Windows Win32K	CVE-2023-41772	8.1
Windows Layer 2 Tunneling Protocol	CVE-2023-41773	8.1
Windows Layer 2 Tunneling Protocol	CVE-2023-41774	8.1

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

- October 2023 release notes

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts