March 12, 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 March 12, 2024, Microsoft published security updates to address vulnerabilities in multiple products. Included were critical updates for the following products:

- Azure Kubernetes Service Confidential Containers – versions prior to 0.3.3
- Microsoft Exchange Server 2016 CU 23 – versions prior to SU12
- Microsoft Exchange Server 2019 CU 13 – versions prior to SU5
- Microsoft Exchange Server 2019 CU 14 – versions prior to SU1
- Microsoft SQL Server backend for Django – versions prior to 1.4.1
- Microsoft System Center Operations Manager (SCOM) 2019 – versions prior to 10.19.1253.0
- Microsoft System Center Operations Manager (SCOM) 2022 – versions prior to 10.22.1070.0
- Open Management Infrastructure – versions prior to 1.8.1-0
- Skype for Consumer – versions prior to 8.113
- Visual Studio Code – versions prior to 1.87.2
- Windows 10 – multiple platforms
- Windows 11 – multiple platforms
- Windows Server – multiple platforms

.

Updated products:

Windows Defender	CVE-2024-20671	5.5
Open Management Infrastructure	CVE-2024-21330	7.8
Open Management Infrastructure	CVE-2024-21334	9.8
Microsoft Authenticator	CVE-2024-21390	7.1
.NET	CVE-2024-21392	7.5
Microsoft Azure Kubernetes Service	CVE-2024-21400	9
Role: Windows Hyper-V	CVE-2024-21407	8.1
Role: Windows Hyper-V	CVE-2024-21408	5.5
Skype for Consumer	CVE-2024-21411	8.8
Software for Open Networking in the Cloud (SONiC)	CVE-2024-21418	7.8
Microsoft Dynamics	CVE-2024-21419	7.6
Azure SDK	CVE-2024-21421	7.5

Microsoft Office SharePoint	CVE-2024-21426	7.8
Windows Kerberos	CVE-2024-21427	7.5
Windows USB Hub Driver	CVE-2024-21429	6.8
Windows USB Serial Driver	CVE-2024-21430	5.7
Windows Hypervisor-Protected Code Integrity	CVE-2024-21431	7.8
Windows Update Stack	CVE-2024-21432	7
Windows Print Spooler Components	CVE-2024-21433	7
Microsoft Windows SCSI Class System File	CVE-2024-21434	7.8
Windows OLE	CVE-2024-21435	8.8
Windows Installer	CVE-2024-21436	7.8
Microsoft Graphics Component	CVE-2024-21437	7.8
Windows AllJoyn API	CVE-2024-21438	7.5
Windows Telephony Server	CVE-2024-21439	7
Windows ODBC Driver	CVE-2024-21440	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21441	8.8
Windows USB Print Driver	CVE-2024-21442	7.8
Windows Kernel	CVE-2024-21443	7.3
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21444	8.8
Windows USB Print Driver	CVE-2024-21445	7
Windows NTFS	CVE-2024-21446	7.8
Microsoft Teams for Android	CVE-2024-21448	5
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21450	8.8
Microsoft WDAC ODBC Driver	CVE-2024-21451	8.8
Windows ODBC Driver	CVE-2024-26159	8.8
Windows Cloud Files Mini Filter Driver	CVE-2024-26160	5.5
Microsoft WDAC OLE DB provider for SQL	CVE-2024-26161	8.8
Windows ODBC Driver	CVE-2024-26162	8.8
SQL Server	CVE-2024-26164	8.8
Visual Studio Code	CVE-2024-26165	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-26166	8.8
Microsoft Edge for Android	CVE-2024-26167	4.3
Windows Error Reporting	CVE-2024-26169	7.8
Windows Composite Image File System	CVE-2024-26170	7.8
Windows Kernel	CVE-2024-26173	7.8
Windows Kernel	CVE-2024-26174	5.5
Windows Kernel	CVE-2024-26176	7.8
Windows Kernel	CVE-2024-26177	5.5
Windows Kernel	CVE-2024-26178	7.8
Windows Kernel	CVE-2024-26181	5.5
Windows Kernel	CVE-2024-26182	7.8
Windows Compressed Folder	CVE-2024-26185	6.5
Microsoft QUIC	CVE-2024-26190	7.5
Windows Standards-Based Storage Management Service	CVE-2024-26197	6.5
Microsoft Exchange Server	CVE-2024-26198	8.8

Microsoft Office	CVE-2024-26199	7.8
Microsoft Intune	CVE-2024-26201	6.6
Azure Data Studio	CVE-2024-26203	7.3
Outlook for Android	CVE-2024-26204	7.5

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

- March 2024 Release Notes
- Security Update Guide