مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Microsoft Products

Tracking #:432315694

Date:13-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Microsoft recently released security updates to patch multiple vulnerabilities in its products.

TECHNICAL DETAILS:

On March 12, 2024, Microsoft released security updates that addressed 60 vulnerabilities, including two critical ones: CVE-2024-21334 (Open Management Infrastructure (OMI) Remote Code Execution Vulnerability) and CVE-2024-21400 (Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability). The updates also addressed two critical issues affecting Windows Hyper-V (CVE-2024-21407 and CVE-2024-21408) that could potentially lead to denial-of-service (DoS) and remote code execution.

Critical and High-Severity Vulnerabilities Details:

Description	CVE	Base Score
Open Management Infrastructure	CVE-2024-21334	9.8
Microsoft Azure Kubernetes Service	CVE-2024-21400	9
Skype for Consumer	CVE-2024-21411	8.8
Windows OLE	CVE-2024-21435	8.8
Windows ODBC Driver	CVE-2024-21440	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21441	8.8
Microsoft WDAC OLE DB provider for SQL	CVE-2024-21444	8.8
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
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 Exchange Server	CVE-2024-26198	8.8
Role: Windows Hyper-V	CVE-2024-21407	8.1
Open Management Infrastructure	CVE-2024-21330	7.8
Software for Open Networking in the Cloud (SONiC)	CVE-2024-21418	7.8
Microsoft Office SharePoint	CVE-2024-21426	7.8
Windows Hypervisor-Protected Code Integrity	CVE-2024-21431	7.8
Microsoft Windows SCSI Class System File	CVE-2024-21434	7.8
Windows Installer	CVE-2024-21436	7.8
Microsoft Graphics Component	CVE-2024-21437	7.8
Windows USB Print Driver	CVE-2024-21442	7.8
Windows NTFS	CVE-2024-21446	7.8
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-2024-26176	7.8
Windows Kernel	CVE-2024-26178	7.8
Windows Kernel	CVE-2024-26182	7.8
Microsoft Office	CVE-2024-26199	7.8
Microsoft Dynamics	CVE-2024-21419	7.6
.NET	CVE-2024-21392	7.5
Azure SDK	CVE-2024-21421	7.5
Windows Kerberos	CVE-2024-21427	7.5
Windows AllJoyn API	CVE-2024-21438	7.5
Microsoft QUIC	CVE-2024-26190	7.5
Outlook for Android	CVE-2024-26204	7.5
Windows Kernel	CVE-2024-21443	7.3
Azure Data Studio	CVE-2024-26203	7.3
Microsoft Authenticator	CVE-2024-21390	7.1
Windows Update Stack	CVE-2024-21432	7
Windows Print Spooler Components	CVE-2024-21433	7
Windows Telephony Server	CVE-2024-21439	7
Windows USB Print Driver	CVE-2024-21445	7

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Microsoft.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://msrc.microsoft.com/update-guide/releaseNote/2024-Mar