

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 November 14, 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
- Azure CLI – multiple platforms

Microsoft has indicated that CVE-2023-36025 and CVE-2023-36036 have been exploited.

These vulnerabilities are rated as an overall **Critical** Severity.

Microsoft Windows Search Component	CVE-2023-36394	7.0
Windows Deployment Services	CVE-2023-36395	7.5
Windows Compressed Folder	CVE-2023-36396	7.8
Windows Internet Connection Sharing (ICS)	CVE-2023-36397	9.8
Windows NTFS	CVE-2023-36398	6.5
Windows Storage	CVE-2023-36399	7.1
Windows HMAC Key Derivation	CVE-2023-36400	8.8
Microsoft Remote Registry Service	CVE-2023-36401	7.2
Microsoft WDAC OLE DB provider for SQL	CVE-2023-36402	8.8
Windows Kernel	CVE-2023-36403	7.0
Windows Kernel	CVE-2023-36404	5.5
Windows Kernel	CVE-2023-36405	7.0
Windows Hyper-V	CVE-2023-36406	5.5
Windows Hyper-V	CVE-2023-36407	7.8
Windows Hyper-V	CVE-2023-36408	7.8
Microsoft Dynamics	CVE-2023-36410	7.6
Microsoft Office	CVE-2023-36413	6.5
Windows Defender	CVE-2023-36422	7.8
Microsoft Remote Registry Service	CVE-2023-36423	7.2
Windows Common Log File System Driver	CVE-2023-36424	7.8
Windows Distributed File System (DFS)	CVE-2023-36425	8.0
Windows Hyper-V	CVE-2023-36427	7.0

Windows Authentication Methods	CVE-2023-36428	5.5
Azure DevOps	CVE-2023-36437	8.8
Microsoft Exchange Server	CVE-2023-36439	8.0
ASP.NET	CVE-2023-36558	6.2
ASP.NET	CVE-2023-36560	8.8
Windows Installer	CVE-2023-36705	7.8
Microsoft Windows Speech	CVE-2023-36719	8.4
Azure	CVE-2023-38151	8.8
Microsoft Office SharePoint	CVE-2023-38177	6.1

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

- [November 2023 Release Notes](#)
- [Security Update Guide](#)

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](#)