**Overall rating: High**

BRITISH COLUMBIA

**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

Updated products:

| | | |
|---|---|---|
| Windows Netlogon | CVE-2023-21526 | 7.4 |
| Microsoft Graphics Component | CVE-2023-21756 | 7.8 |
| Windows Admin Center | CVE-2023-29347 | 8.7 |
| Windows Cluster Server | CVE-2023-32033 | 6.6 |
| Windows Remote Procedure Call | CVE-2023-32034 | 6.5 |
| Windows Remote Procedure Call | CVE-2023-32035 | 6.5 |
| Windows Layer 2 Tunneling Protocol | CVE-2023-32037 | 6.5 |
| Windows ODBC Driver | CVE-2023-32038 | 8.8 |
| Microsoft Printer Drivers | CVE-2023-32039 | 5.5 |
| Microsoft Printer Drivers | CVE-2023-32040 | 5.5 |
| Windows Update Orchestrator Service | CVE-2023-32041 | 5.5 |
| Windows OLE | CVE-2023-32042 | 6.5 |
| Windows Remote Desktop | CVE-2023-32043 | 6.8 |
| Windows Message Queuing | CVE-2023-32044 | 7.5 |
| Windows Message Queuing | CVE-2023-32045 | 7.5 |
| Windows MSHTML Platform | CVE-2023-32046 | 7.8 |
| Paint 3D | CVE-2023-32047 | 7.8 |
| Windows SmartScreen | CVE-2023-32049 | 8.8 |
| Windows Installer | CVE-2023-32050 | 7.0 |
| Microsoft Windows Codecs Library | CVE-2023-32051 | 7.8 |
| Microsoft Power Apps | CVE-2023-32052 | 6.3 |
| Windows Installer | CVE-2023-32053 | 7.8 |
| Windows Volume Shadow Copy | CVE-2023-32054 | 7.3 |
| Windows Active Template Library | CVE-2023-32055 | 6.7 |
| Windows Server Update Service | CVE-2023-32056 | 7.8 |
| Windows Message Queuing | CVE-2023-32057 | 9.8 |
| Windows Failover Cluster | CVE-2023-32083 | 6.5 |
| Windows HTTP.sys | CVE-2023-32084 | 7.5 |
| Microsoft Printer Drivers | CVE-2023-32085 | 5.5 |
| .NET and Visual Studio | CVE-2023-33127 | 8.1 |
| Microsoft Office SharePoint | CVE-2023-33134 | 8.8 |
| Microsoft Office | CVE-2023-33148 | 7.8 |

| | | |
|---|---|---|
| Microsoft Graphics Component | CVE-2023-33149 | 7.8 |
| Microsoft Office | CVE-2023-33150 | 9.6 |
| Microsoft Office Outlook | CVE-2023-33151 | 6.5 |
| Microsoft Office Access | CVE-2023-33152 | 7.0 |
| Microsoft Office Outlook | CVE-2023-33153 | 6.8 |
| Windows Partition Management Driver | CVE-2023-33154 | 7.8 |
| Windows Cloud Files Mini Filter Driver | CVE-2023-33155 | 7.8 |
| Windows Defender | CVE-2023-33156 | 6.3 |
| Microsoft Office SharePoint | CVE-2023-33157 | 8.8 |
| Microsoft Office Excel | CVE-2023-33158 | 7.8 |
| Microsoft Office SharePoint | CVE-2023-33159 | 8.8 |
| Microsoft Office SharePoint | CVE-2023-33160 | 8.8 |
| Microsoft Office Excel | CVE-2023-33161 | 7.8 |
| Microsoft Office Excel | CVE-2023-33162 | 5.5 |
| Windows Network Load Balancing | CVE-2023-33163 | 7.5 |
| Windows Remote Procedure Call | CVE-2023-33164 | 6.5 |
| Microsoft Office SharePoint | CVE-2023-33165 | 4.3 |
| Windows Remote Procedure Call | CVE-2023-33166 | 6.5 |
| Windows Remote Procedure Call | CVE-2023-33167 | 6.5 |
| Windows Remote Procedure Call | CVE-2023-33168 | 6.5 |
| Windows Remote Procedure Call | CVE-2023-33169 | 6.5 |
| ASP.NET and .NET | CVE-2023-33170 | 8.1 |
| Microsoft Dynamics | CVE-2023-33171 | 6.1 |
| Windows Remote Procedure Call | CVE-2023-33172 | 6.5 |
| Windows Remote Procedure Call | CVE-2023-33173 | 6.5 |
| Windows Cryptographic Services | CVE-2023-33174 | 5.5 |
| Microsoft Printer Drivers | CVE-2023-35296 | 6.5 |
| Windows PGM | CVE-2023-35297 | 7.5 |
| Windows HTTP.sys | CVE-2023-35298 | 7.5 |
| Windows Common Log File System Driver | CVE-2023-35299 | 7.8 |
| Windows Remote Procedure Call | CVE-2023-35300 | 8.8 |
| Microsoft Printer Drivers | CVE-2023-35302 | 8.8 |
| Microsoft Windows Codecs Library | CVE-2023-35303 | 8.8 |
| Windows Kernel | CVE-2023-35304 | 7.8 |
| Windows Kernel | CVE-2023-35305 | 7.8 |
| Microsoft Printer Drivers | CVE-2023-35306 | 5.5 |
| Windows MSHTML Platform | CVE-2023-35308 | 4.4 |
| Windows Message Queuing | CVE-2023-35309 | 7.5 |
| Role: DNS Server | CVE-2023-35310 | 6.6 |
| Microsoft Office Outlook | CVE-2023-35311 | 8.8 |
| Windows VOLSNAP.SYS | CVE-2023-35312 | 7.3 |
| Windows Online Certificate Status Protocol (OCSP) SnapIn | CVE-2023-35313 | 6.7 |
| Windows Remote Procedure Call | CVE-2023-35314 | 5.3 |
| Windows Layer-2 Bridge Network Driver | CVE-2023-35315 | 8.8 |

| | | |
|---|---|---|
| Windows Remote Procedure Call | CVE-2023-35316 | 6.5 |
| Windows Server Update Service | CVE-2023-35317 | 7.8 |
| Windows Remote Procedure Call | CVE-2023-35318 | 6.5 |
| Windows Remote Procedure Call | CVE-2023-35319 | 6.5 |
| Windows Connected User Experiences and Telemetry | CVE-2023-35320 | 7.8 |
| Windows Deployment Services | CVE-2023-35321 | 6.5 |
| Windows Deployment Services | CVE-2023-35322 | 8.8 |
| Windows Online Certificate Status Protocol (OCSP) SnapIn | CVE-2023-35323 | 7.8 |
| Microsoft Printer Drivers | CVE-2023-35324 | 5.5 |
| Windows Print Spooler Components | CVE-2023-35325 | 7.5 |
| Windows CDP User Components | CVE-2023-35326 | 5.5 |
| Windows Transaction Manager | CVE-2023-35328 | 7.8 |
| Windows Authentication Methods | CVE-2023-35329 | 6.5 |
| Windows SPNEGO Extended Negotiation | CVE-2023-35330 | 6.2 |
| Windows Local Security Authority (LSA) | CVE-2023-35331 | 6.5 |
| Windows Remote Desktop | CVE-2023-35332 | 6.8 |
| Microsoft Media-Wiki Extensions | CVE-2023-35333 | 7.1 |
| Microsoft Dynamics | CVE-2023-35335 | 8.2 |
| Windows MSHTML Platform | CVE-2023-35336 | 6.5 |
| Windows Win32K | CVE-2023-35337 | 7.8 |
| Windows Peer Name Resolution Protocol | CVE-2023-35338 | 7.5 |
| Windows CryptoAPI | CVE-2023-35339 | 7.5 |
| Windows CNG Key Isolation Service | CVE-2023-35340 | 7.8 |
| Windows Media | CVE-2023-35341 | 6.2 |
| Windows Image Acquisition | CVE-2023-35342 | 7.8 |
| Windows Geolocation Service | CVE-2023-35343 | 7.8 |
| Role: DNS Server | CVE-2023-35344 | 6.6 |
| Role: DNS Server | CVE-2023-35345 | 6.6 |
| Role: DNS Server | CVE-2023-35346 | 6.6 |
| Windows App Store | CVE-2023-35347 | 7.1 |
| Azure Active Directory | CVE-2023-35348 | 7.5 |
| Windows Active Directory Certificate Services | CVE-2023-35350 | 7.2 |
| Windows Active Directory Certificate Services | CVE-2023-35351 | 6.6 |
| Windows Remote Desktop | CVE-2023-35352 | 7.5 |
| Windows Connected User Experiences and Telemetry | CVE-2023-35353 | 7.8 |
| Windows Kernel | CVE-2023-35356 | 7.8 |
| Windows Kernel | CVE-2023-35357 | 7.8 |
| Windows Kernel | CVE-2023-35358 | 7.8 |
| Windows NT OS Kernel | CVE-2023-35360 | 7.0 |
| Windows NT OS Kernel | CVE-2023-35361 | 7.0 |
| Windows Clip Service | CVE-2023-35362 | 7.8 |
| Windows Kernel | CVE-2023-35363 | 7.8 |
| Windows NT OS Kernel | CVE-2023-35364 | 8.8 |
| Windows Routing and Remote Access Service (RRAS) | CVE-2023-35365 | 9.8 |

| | | |
|---|---|---|
| Windows Routing and Remote Access Service (RRAS) | CVE-2023-35366 | 9.8 |
| Windows Routing and Remote Access Service (RRAS) | CVE-2023-35367 | 9.8 |
| Mono Authenticode | CVE-2023-35373 | 5.3 |
| Paint 3D | CVE-2023-35374 | 7.8 |
| Visual Studio Code | CVE-2023-36867 | 7.8 |
| Service Fabric | CVE-2023-36868 | 6.5 |
| Azure Active Directory | CVE-2023-36871 | 6.5 |
| Microsoft Windows Codecs Library | CVE-2023-36872 | 5.5 |
| Windows Error Reporting | CVE-2023-36874 | 7.8 |
| Microsoft Office | CVE-2023-36884 | 8.3 |

These vulnerabilities are rated as an overall **High** 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

- July 2023 Release Notes
- Security Update Guide