ADV2026_82 Microsoft Security Advisory - Monthly Rollup – Update 1 (February 15th, 2026)

Microsoft published a security advisory highlighting vulnerabilities in the following products on February 10, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- .NET 10.0
- .NET 8.0
- .NET 9.0
- Azure AI Language Authoring
- Azure ARC
- Azure DevOps Server 2022
- Azure Front Door
- Azure Functions
- Azure HDInsight
- Azure IoT Explorer
- Azure Local
- GitHub Copilot Plugin for JetBrains IDEs
- Microsoft 365
- Microsoft ACI Confidential Containers
- Microsoft Defender for Endpoint for Linux
- Microsoft Excel 2016
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft Exchange Server Subscription Edition RTM
- Microsoft Office 2019
- Microsoft Office LTSC
- Microsoft Office LTSC 2021
- Microsoft Office LTSC 2024
- Microsoft Outlook 2016

- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft SQL Server 2022
- Microsoft SQL Server 2025
- Microsoft Visual Studio 2022
- Microsoft Word 2016
- Office Online Server
- Power BI Report Server
- Visual Studio Code
- Windows 10
- Windows 11
- Windows App for Mac
- Windows Notepad
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Microsoft has received reports that CVE-2026-21525, CVE-2026-21514, CVE-2026-21510, CVE-2026-21513, CVE-2026-21533 and CVE-2026-21519 are being exploited.

Update 1

CVE-2026-21525, CVE-2026-21514, CVE-2026-21510, CVE-2026-21513, CVE-2026-21533 and CVE-2026-21519 were added to the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) Database on February 10, 2026.

For more information on these updates, you can follow these URLs:

- February 2026 Security Updates
- Security Update Guide
- CISA KEV: CVE-2026-21510
- CISA KEV: CVE-2026-21513
- CISA KEV: CVE-2026-21514
- CISA KEV: CVE-2026-21519
- CISA KEV: CVE-2026-21525
- CISA KEV: CVE-2026-21533

The Guyana National CIRT recommends that users and administrators review this update and apply it where necessary.

References

- CISA KEV: CVE-2026-21510. (n.d). Retrieved from Microsoft. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-21510

- CISA KEV: CVE-2026-21514. (n.d). Retrieved from Microsoft. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-21514

- CISA KEV: CVE-2026-21519. (n.d). Retrieved from Microsoft. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-21519

- CISA KEV: CVE-2026-21525. (n.d). Retrieved from Microsoft. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-21525

- CISA KEV: CVE-2026-21533. (n.d). Retrieved from Microsoft. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-21525 https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-21533

- February 2026 Security Updates. (n.d). Retrieved from Microsoft. https://msrc.microsoft.com/update-guide/releaseNote/2026-Feb

- Microsoft security advisory (February 13, 2026). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/microsoft-security-advisory-february-2026-monthly-rollup-av26-111