

| | CVE番号 | 記述 | 深刻度 | CVSS | 周知されたか | 悪用されたか | 脆弱性タイプ |
|----|----------------------------------|--|-----|------|--------|--------|----------------|
| 1 | CVE-2026-21514 | Microsoft Word セキュリティ機能バイパス脆弱性 | 重要 | 7.8 | Yes | Yes | セキュリティ機能バイパス |
| 2 | CVE-2026-21510 | Windows Shell セキュリティ機能バイパス脆弱性 | 重要 | 8.8 | Yes | Yes | セキュリティ機能バイパス |
| 3 | CVE-2026-21513 | Internet Explorer セキュリティ機能バイパス脆弱性 | 重要 | 8.8 | Yes | Yes | セキュリティ機能バイパス |
| 4 | CVE-2026-21519 | デスクトップウィンドウマネージャー特権昇格脆弱性 | 重要 | 7.8 | No | Yes | 特権昇格 |
| 5 | CVE-2026-21533 | Windows リモートデスクトップサービス特権昇格脆弱性 | 重要 | 7.8 | No | Yes | 特権昇格 |
| 6 | CVE-2026-21525 | Windows リモートアクセス接続マネージャーサービス拒否脆弱性 | 警告 | 6.2 | No | Yes | DoS攻撃 |
| 7 | CVE-2026-21511 | Microsoft Outlook なりすまし脆弱性 | 重要 | 7.5 | No | No | なりすまし |
| 8 | CVE-2023-2804 * | Red Hat, Inc. CVE-2023-2804: libjpeg-turbo のヒープベースのオーバーフロー | 重要 | 6.5 | Yes | No | リモートコード実行 |
| 9 | CVE-2026-24302 | Azure Arc の特権昇格の脆弱性 | 緊急 | 8.6 | No | No | 特権昇格 |
| 10 | CVE-2026-24300 | Azure Front Door の特権昇格の脆弱性 | 緊急 | 9.8 | No | No | 特権昇格 |
| 11 | CVE-2026-21532 | Azure Function の情報漏洩の脆弱性 | 緊急 | 8.2 | No | No | 情報漏洩 |
| 12 | CVE-2026-21522 | Microsoft ACI Confidential Containers の特権昇格の脆弱性 | 緊急 | 6.7 | No | No | 特権昇格 |
| 13 | CVE-2026-23655 | Microsoft ACI Confidential Containers の情報漏洩の脆弱性 | 緊急 | 6.5 | No | No | 情報漏洩 |
| 14 | CVE-2026-21218 | .NET および Visual Studio のなりすましの脆弱性 | 重要 | 7.5 | No | No | なりすまし |
| 15 | CVE-2026-21512 | Azure DevOps Server クロスサイトスクリプティング脆弱性 | 重要 | 6.5 | No | No | クロスサイトスクリプティング |
| 16 | CVE-2026-21529 † | Azure HDInsight なりすまし脆弱性 | 重要 | 5.7 | No | No | なりすまし |
| 17 | CVE-2026-21528 | Azure IoT Explorer 情報漏洩脆弱性 | 重要 | 6.5 | No | No | 情報漏洩 |
| 18 | CVE-2026-21228 | Azure Local リモートコード実行脆弱性 | 重要 | 8.1 | No | No | リモートコード実行 |
| 19 | CVE-2026-21531 | Python用Azure SDK リモートコード実行脆弱性 | 重要 | 9.8 | No | No | リモートコード実行 |
| 20 | CVE-2026-21251 | クラスタークライアントフェイルオーバー(CCF) 特権昇格脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 21 | CVE-2026-20846 | GDI+ サービス拒否脆弱性 | 重要 | 7.5 | No | No | DoS攻撃 |
| 22 | CVE-2026-21523 | GitHub Copilot および Visual Studio Code リモートコード実行の脆弱性 | 重要 | 8 | No | No | リモートコード実行 |
| 23 | CVE-2026-21518 | GitHub Copilot および Visual Studio Code セキュリティ機能バイパスの脆弱性 | 重要 | 6.5 | No | No | セキュリティ機能バイパス |
| 24 | CVE-2026-21257 | GitHub Copilot および Visual Studio 特権昇格の脆弱性 | 重要 | 8 | No | No | 特権昇格 |
| 25 | CVE-2026-21256 | GitHub Copilot および Visual Studio リモートコード実行の脆弱性 | 重要 | 8.8 | No | No | リモートコード実行 |
| 26 | CVE-2026-21516 | Jetbrains向けGitHub Copilot リモートコード実行の脆弱性 | 重要 | 8.8 | No | No | リモートコード実行 |
| 27 | CVE-2026-21253 | Mailslotファイルシステム 特権昇格の脆弱性 | 重要 | 7 | No | No | 特権昇格 |
| 28 | CVE-2026-21537 † | Microsoft Defender for Endpoint Linux拡張 リモートコード実行の脆弱性 | 重要 | 8.8 | No | No | リモートコード実行 |
| 29 | CVE-2026-21259 | Microsoft Excel 特権昇格の脆弱性 | 重要 | 7.3 | No | No | 特権昇格 |
| 30 | CVE-2026-21258 | Microsoft Excel 情報漏洩の脆弱性 | 重要 | 5.5 | No | No | 情報漏洩 |
| 31 | CVE-2026-21261 | Microsoft Excel 情報漏洩の脆弱性 | 重要 | 5.5 | No | No | 情報漏洩 |
| 32 | CVE-2026-21527 | Microsoft Exchange Server なりすましの脆弱性 | 重要 | 6.5 | No | No | なりすまし |
| 33 | CVE-2026-21260 | Microsoft Outlook なりすまし脆弱性 | 重要 | 7.5 | No | No | なりすまし |
| 34 | CVE-2026-21229 | Power BI リモートコード実行脆弱性 | 重要 | 8 | No | No | リモートコード実行 |
| 35 | CVE-2026-21236 | Windows WinSock 補助機能ドライバート権昇格脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 36 | CVE-2026-21238 | Windows WinSock 補助機能ドライバート権昇格脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 37 | CVE-2026-21241 | Windows WinSock 補助機能ドライバート権昇格脆弱性 | 重要 | 7 | No | No | 特権昇格 |
| 38 | CVE-2026-21517 | Windows for Mac インストーラート権昇格脆弱性 | 重要 | 7 | No | No | 特権昇格 |
| 39 | CVE-2026-21234 | Windows 接続デバイス プラットフォーム サービスの特権昇格の脆弱性 | 重要 | 7 | No | No | 特権昇格 |
| 40 | CVE-2026-21235 | Windows グラフィックス コンポーネントの特権昇格の脆弱性 | 重要 | 7.3 | No | No | 特権昇格 |
| 41 | CVE-2026-21246 | Windows グラフィックス コンポーネントの特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 42 | CVE-2026-21232 | Windows HTTP.sys の特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 43 | CVE-2026-21240 | Windows HTTP.sys の特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |

| | | | | | | | |
|----|---------------------------------|---|----|-----|----|----|--------------|
| 44 | CVE-2026-21250 | Windows HTTP.sysの特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 45 | CVE-2026-21244 | Windows Hyper-Vのリモートコード実行の脆弱性 | 重要 | 7.3 | No | No | リモートコード実行 |
| 46 | CVE-2026-21247 | Windows Hyper-Vリモートコード実行の脆弱性 | 重要 | 7.3 | No | No | リモートコード実行 |
| 47 | CVE-2026-21248 | Windows Hyper-Vリモートコード実行の脆弱性 | 重要 | 7.3 | No | No | リモートコード実行 |
| 48 | CVE-2026-21255 | Windows Hyper-Vセキュリティ機能バイパスの脆弱性 | 重要 | 8.8 | No | No | セキュリティ機能バイパス |
| 49 | CVE-2026-21231 | Windows カーネル特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 50 | CVE-2026-21239 | Windows カーネル特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 51 | CVE-2026-21245 | Windows カーネル特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 52 | CVE-2026-21222 | Windows カーネル情報漏洩の脆弱性 | 重要 | 5.5 | No | No | 情報漏洩 |
| 53 | CVE-2026-21243 | Windows 軽量ディレクトリアクセスプロトコル (LDAP) サービス拒否脆弱性 | 重要 | 7.5 | No | No | DoS攻撃 |
| 54 | CVE-2026-20841 | Windows メモ帳アプリリモートコード実行脆弱性 | 重要 | 8.8 | No | No | リモートコード実行 |
| 55 | CVE-2026-21249 | Windows NTLM スプーフィング脆弱性 | 重要 | 3.3 | No | No | なりすまし |
| 56 | CVE-2026-21508 | Windows ストレージ特権昇格脆弱性 | 重要 | 7 | No | No | 特権昇格 |
| 57 | CVE-2026-21237 | Windows Subsystem for Linux 特権昇格脆弱性 | 重要 | 7 | No | No | 特権昇格 |
| 58 | CVE-2026-21242 | Windows Subsystem for Linux 特権昇格脆弱性 | 重要 | 7 | No | No | 特権昇格 |
| 59 | CVE-2026-1861 * | Chromium: CVE-2026-1861 libvpx におけるヒープバッファオーバーフロー | 高 | N/A | No | No | リモートコード実行 |
| 60 | CVE-2026-1862 * | Chromium: CVE-2026-1862 V8 における型混同 | 高 | N/A | No | No | リモートコード実行 |
| 61 | CVE-2026-0391 | Android 向け Microsoft Edge (Chromium ベース) スプーフィング脆弱性 | 警告 | 6.5 | No | No | なりすまし |