

| 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-2024-30051 Windows DWM コアライブラリにおける特権昇格の脆弱性 | 重要 | 7.8 | Yes | Yes | 特権昇格 |
| 2 | CVE-2024-30040 Windows MSHTML プラットフォームのセキュリティ機能バイパスの脆弱性 | 重要 | 8.8 | No | Yes | セキュリティ機能バイパス |
| 3 | CVE-2024-30046 ASP.NET Core DoS攻撃の脆弱性 | 重要 | 5.9 | Yes | No | DoS攻撃 |
| 4 | CVE-2024-30044 Microsoft SharePoint Server リモートコード実行の脆弱性 | 緊急 | 8.8 | No | No | リモートコード実行 |
| 5 | CVE-2024-30045 .NET および Visual Studio のリモートコード実行の脆弱性 | 重要 | 6.3 | No | No | リモートコード実行 |
| 6 | CVE-2024-30053 Azure Migrate スプーフィング脆弱性 | 重要 | 7.5 | No | No | なりすまし |
| 7 | CVE-2024-32002 * CVE-2023-32002 シンボリックリンクをサポートする大文字小文字を区別しないファイルシステム上の再帰的クローンにリモートコード実行の脆弱性 | 重要 | 9.8 | No | No | リモートコード実行 |
| 8 | CVE-2024-30019 DHCP サーバサービスにDoS攻撃の脆弱性 | 重要 | 6.5 | No | No | DoS攻撃 |
| 9 | CVE-2024-30047 Dynamics 365 Customer Insights になりすましの脆弱性 | 重要 | 7.6 | No | No | なりすまし |
| 10 | CVE-2024-30048 Dynamics 365 Customer Insights になりすましの脆弱性 | 重要 | 7.6 | No | No | なりすまし |
| 11 | CVE-2024-32004 * GitHub CVE-2024-32004 GitHub : CVE-2023-32004 特別な細工を施したローカルポジトリのクローン作成時にリモートでコードが実行される脆弱性 | 重要 | 8.8 | No | No | リモートコード実行 |
| 12 | CVE-2024-30041 Microsoft Bing Search になりすましの脆弱性 | 重要 | 5.4 | No | No | なりすまし |
| 13 | CVE-2024-30007 Microsoft Brokering File System における特権昇格の脆弱性 | 重要 | 8.8 | No | No | 特権昇格 |
| 14 | CVE-2024-30042 Microsoft Excel リモートコード実行の脆弱性 | 重要 | 7.8 | No | No | リモートコード実行 |
| 15 | CVE-2024-26238 Microsoft PLUGScheduler スケジューラによる特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 16 | CVE-2024-30054 Microsoft Power BI Client Javascript SDK 情報漏えいの脆弱性 | 重要 | 6.5 | No | No | 情報漏えい |
| 17 | CVE-2024-30043 Microsoft SharePoint Server 情報漏えいの脆弱性 | 重要 | 6.5 | No | No | 情報漏えい |
| 18 | CVE-2024-30006 Microsoft WDAC OLE DB provider for SQL Server 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 |
| 19 | CVE-2024-29994 Microsoft Windows SCSI クラスシステムファイルにおける特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 20 | CVE-2024-30027 NTFS における特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 21 | CVE-2024-30028 Win32k における特権の昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 22 | CVE-2024-30030 Win32k 権限昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 23 | CVE-2024-30038 Win32k における特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 24 | CVE-2024-30034 Windows Cloud Files Mini Filter ドライバ情報漏えいの脆弱性 | 重要 | 5.5 | No | No | 情報漏えい |
| 25 | CVE-2024-30031 Windows CNG Key Isolation Service 権限昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 26 | CVE-2024-29996 Windows Common Log File System ドライバの特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 27 | CVE-2024-30025 Windows 共通ログファイルシステムドライバの特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 28 | CVE-2024-30037 Windows 共通ログファイルシステムドライバの特権昇格の脆弱性 | 重要 | 7.5 | No | No | 特権昇格 |
| 29 | CVE-2024-30016 Windows 暗号化サービス情報漏えいの脆弱性 | 重要 | 5.5 | No | No | 情報漏えい |
| 30 | CVE-2024-30020 Windows 暗号化サービス リモートコード実行の脆弱性 | 重要 | 8.1 | No | No | リモートコード実行 |
| 31 | CVE-2024-30036 Windows デプロイメントサービス情報漏えいの脆弱性 | 重要 | 6.5 | No | No | 情報漏えい |
| 32 | CVE-2024-30032 Windows DWM コアライブラリの特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 33 | CVE-2024-30035 Windows DWM コアライブラリの特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 34 | CVE-2024-30008 Windows DWM コアライブラリ情報漏えいの脆弱性 | 重要 | 5.5 | No | No | 情報漏えい |
| 35 | CVE-2024-30011 Windows Hyper-V DoS攻撃の脆弱性 | 重要 | 6.5 | No | No | DoS攻撃 |
| 36 | CVE-2024-30010 Windows Hyper-V 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 |
| 37 | CVE-2024-30017 Windows Hyper-V 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 |
| 38 | CVE-2024-30018 Windows カーネル特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 39 | CVE-2024-29997 Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |
| 40 | CVE-2024-29998 Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |
| 41 | CVE-2024-29999 Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |
| 42 | CVE-2024-30000 Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |
| 43 | CVE-2024-30001 Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |
| 44 | CVE-2024-30002 Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |
| 45 | CVE-2024-30003 Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |
| 46 | CVE-2024-30004 Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |

| | | | | | | | |
|----|---------------------------------|--|----|-----|----|----|--------------|
| 47 | CVE-2024-30005 | Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |
| 48 | CVE-2024-30012 | Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |
| 49 | CVE-2024-30021 | Windows Mobile Broadband ドライバのリモートコード実行の脆弱性 | 重要 | 6.8 | No | No | リモートコード実行 |
| 50 | CVE-2024-30039 | Windows リモートアクセス接続マネージャ情報漏洩の脆弱性 | 重要 | 5.5 | No | No | 情報漏えい |
| 51 | CVE-2024-30009 | Windows Routing and Remote Access Service (RRAS) 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 |
| 52 | CVE-2024-30014 | Windows Routing and Remote Access Service (RRAS) リモートコード実行の脆弱性 | 重要 | 7.5 | No | No | リモートコード実行 |
| 53 | CVE-2024-30015 | Windows Routing and Remote Access Service (RRAS) リモートコード実行の脆弱性 | 重要 | 7.5 | No | No | リモートコード実行 |
| 54 | CVE-2024-30022 | Windows Routing and Remote Access Service (RRAS) リモートコード実行の脆弱性 | 重要 | 7.5 | No | No | リモートコード実行 |
| 55 | CVE-2024-30023 | Windows Routing and Remote Access Service (RRAS) リモートコード実行の脆弱性 | 重要 | 7.5 | No | No | リモートコード実行 |
| 56 | CVE-2024-30024 | Windows Routing and Remote Access Service (RRAS) リモートコード実行の脆弱性 | 重要 | 7.5 | No | No | リモートコード実行 |
| 57 | CVE-2024-30029 | Windows Routing and Remote Access Service (RRAS) リモートコード実行の脆弱性 | 重要 | 7.5 | No | No | リモートコード実行 |
| 58 | CVE-2024-30033 | Windows Search Service における特権昇格の脆弱性 | 重要 | 7 | No | No | 特権昇格 |
| 59 | CVE-2024-30049 | Windows Win32 カーネルサブシステムの特権昇格の脆弱性 | 重要 | 7.8 | No | No | 特権昇格 |
| 60 | CVE-2024-30059 | Microsoft Intune for Android モバイルアプリケーション管理改ざんの脆弱性 | 重要 | 6.1 | No | No | 改ざん |
| 61 | CVE-2024-30050 | Windows Mark of the Web セキュリティ機能バイパスの脆弱性 | 警告 | 5.4 | No | No | セキュリティ機能バイパス |
| 62 | CVE-2024-4331 * | Chromium CVE-2024-4331 Picture In Picture におけるユース・アフター・フリーの脆弱性 | 高 | N/A | No | No | リモートコード実行 |
| 63 | CVE-2024-4368 * | Chromium CVE-2024-4368 Dawn におけるユース・アフター・フリーの脆弱性 | 高 | N/A | No | No | リモートコード実行 |

*サードパーティによってリリースされ、現在Microsoftのリリースに含まれていることを示す。

†脆弱性に完全に対処するために、インストール後の対応が必要であることを示す。