

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-2026-20805 デスクトップウィンドウマネージャー情報漏洩脆弱性	重要	5.5	No	Yes	情報漏洩
2	CVE-2023-31096 * MITRE: CVE-2023-31096 Windows Agere ソフトモデムドライバー特権昇格脆弱性	重要	7.8	Yes	No	特権昇格
3	CVE-2026-21265 † セキュアブート証明書有効期限切れセキュリティ機能バイパス脆弱性	重要	6.4	Yes	No	セキュリティ機能バイパス
4	CVE-2024-55414 * Windows Motorola ソフトモデムドライバー特権昇格脆弱性	重要	7.8	Yes*	No	特権昇格
5	CVE-2026-20955 Microsoft Excel リモートコード実行の脆弱性	緊急	7.8	No	No	リモートコード実行
6	CVE-2026-20957 Microsoft Excel リモートコード実行の脆弱性	緊急	7.8	No	No	リモートコード実行
7	CVE-2026-20952 Microsoft Office リモートコード実行の脆弱性	緊急	8.4	No	No	リモートコード実行
8	CVE-2026-20953 Microsoft Office リモートコード実行の脆弱性	緊急	8.4	No	No	リモートコード実行
9	CVE-2026-20944 Microsoft Word リモートコード実行の脆弱性	緊急	7.8	No	No	リモートコード実行
10	CVE-2026-20822 Windows グラフィックスコンポーネント特権昇格の脆弱性	緊急	7.8	No	No	特権昇格
11	CVE-2026-20854 Windows オールセキュリティオーソリティサブシステムサービス (LSASS) リモートコード実行の脆弱性	緊急	7.5	No	No	リモートコード実行
12	CVE-2026-20876 Windows 仮想化ベースのセキュリティ (VBS) エンクレープ特権昇格の脆弱性	緊急	6.7	No	No	特権昇格
13	CVE-2026-21224 Azure Connected Machine Agent 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
14	CVE-2026-21226 Python 用 Azure Core 共有クライアントライブラリ 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
15	CVE-2026-20815 機能アクセス管理サービス (camsvc) 特権昇格の脆弱性	重要	7	No	No	特権昇格
16	CVE-2026-20830 機能アクセス管理サービス (camsvc) 特権昇格の脆弱性	重要	7	No	No	特権昇格
17	CVE-2026-21221 機能アクセス管理サービス (camsvc) の特権昇格の脆弱性	重要	7	No	No	特権昇格
18	CVE-2026-20835 機能アクセス管理サービス (camsvc) の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
19	CVE-2026-20851 機能アクセス管理サービス (camsvc) の情報漏洩の脆弱性	重要	6.2	No	No	情報漏洩
20	CVE-2026-20871 デスクトップ Windows マネージャーの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
21	CVE-2026-20814 DirectX グラフィックスカーネルの特権昇格の脆弱性	重要	7	No	No	特権昇格
22	CVE-2026-20836 DirectX グラフィックスカーネルの特権昇格の脆弱性	重要	7	No	No	特権昇格
23	CVE-2026-20962 測定用動的信頼の根源 (DRTM) 情報漏洩の脆弱性	重要	4.4	No	No	情報漏洩
24	CVE-2026-20941 Windows タスク用ホストプロセス 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
25	CVE-2026-21219 インボックス COM オブジェクト (グローバルメモリ) リモートコード実行の脆弱性	重要	7	No	No	リモートコード実行
26	CVE-2026-20812 LDAP改ざん脆弱性	重要	6.5	No	No	改ざん
27	CVE-2026-20842 Microsoft DWMコアライブラリ特権昇格脆弱性	重要	7	No	No	特権昇格
28	CVE-2026-20946 Microsoft Excel リモートコード実行脆弱性	重要	7.8	No	No	リモートコード実行
29	CVE-2026-20950 Microsoft Excel リモートコード実行脆弱性	重要	7.8	No	No	リモートコード実行
30	CVE-2026-20956 Microsoft Excel リモートコード実行脆弱性	重要	7.8	No	No	リモートコード実行
31	CVE-2026-20949 Microsoft Excelセキュリティ機能バイパス脆弱性	重要	7.8	No	No	セキュリティ機能バイパス
32	CVE-2026-20943 Microsoft Office Click-To-Run特権昇格脆弱性	重要	7	No	No	特権昇格
33	CVE-2026-20958 Microsoft SharePoint情報漏洩脆弱性	重要	5.4	No	No	情報漏洩
34	CVE-2026-20963 Microsoft SharePoint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
35	CVE-2026-20947 Microsoft SharePoint 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
36	CVE-2026-20951 Microsoft SharePoint Server 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
37	CVE-2026-20959 Microsoft SharePoint Server なりすましの脆弱性	重要	4.6	No	No	なりすまし
38	CVE-2026-20803 † Microsoft SQL Server 特権昇格の脆弱性	重要	7.2	No	No	特権昇格
39	CVE-2026-20847 Microsoft Windows ファイルエクスプローラー なりすましの脆弱性	重要	6.5	No	No	なりすまし
40	CVE-2026-20948 Microsoft Word 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
41	CVE-2026-20872 NTLMハッシュ開示なりすましの脆弱性	重要	6.5	No	No	なりすまし
42	CVE-2026-20925 NTLMハッシュ開示なりすましの脆弱性	重要	6.5	No	No	なりすまし
43	CVE-2026-20821 リモートプロシージャコール情報開示の脆弱性	重要	6.2	No	No	情報漏洩
44	CVE-2026-20826 タブレット Windows ユーザー インターフェイス (TWINUI) サブシステム 情報漏洩脆弱性	重要	7.8	No	No	特権昇格

45	CVE-2026-20827	タブレット Windows ユーザー インターフェイス (TWINUI) サブシステム 情報漏洩脆弱性	重要	5.5	No	No	情報漏洩
46	CVE-2026-20829	TPM トラストレット 情報漏洩脆弱性	重要	5.5	No	No	情報漏洩
47	CVE-2026-20811	Win32k 特権昇格脆弱性	重要	7.8	No	No	特権昇格
48	CVE-2026-20863	Win32k 特権昇格脆弱性	重要	7	No	No	特権昇格
49	CVE-2026-20920	Win32k 特権昇格脆弱性	重要	7.8	No	No	特権昇格
50	CVE-2026-20965	Windows Admin Center 特権昇格の脆弱性	重要	7.5	No	No	特権昇格
51	CVE-2026-20810	Windows WinSock 補助機能ドライバ 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
52	CVE-2026-20831	Windows WinSock 補助機能ドライバ 特権昇格の脆弱性	重要	7	No	No	特権昇格
53	CVE-2026-20860	Windows WinSock 補助機能ドライバ 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
54	CVE-2026-20839	Windows クライアント側キャッシュ (CSC) サービス 情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
55	CVE-2026-20844	Windows キーボード サーバーの特権昇格の脆弱性	重要	7.4	No	No	特権昇格
56	CVE-2026-20857	Windows クラウドファイル ミニ フィルター ドライバーの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
57	CVE-2026-20940	Windows クラウドファイル ミニ フィルター ドライバーの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
58	CVE-2026-20820	Windows 共通ログファイル システム ドライバーの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
59	CVE-2026-20864	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	7.8	No	No	特権昇格
60	CVE-2026-0386 †	Windows 展開サービスのリモート コード実行の脆弱性	重要	7.5	No	No	リモートコード実行
61	CVE-2026-20817	Windows エラー報告サービス特権昇格の脆弱性	重要	7.8	No	No	特権昇格
62	CVE-2026-20808	Windows ファイル エクスプローラー特権昇格の脆弱性	重要	7	No	No	特権昇格
63	CVE-2026-20823	Windows ファイル エクスプローラー情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
64	CVE-2026-20932	Windows ファイル エクスプローラー情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
65	CVE-2026-20937	Windows ファイル エクスプローラー情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
66	CVE-2026-20939	Windows ファイル エクスプローラー情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
67	CVE-2026-20804	Windows Hello 改ざんの脆弱性	重要	7.7	No	No	改ざん
68	CVE-2026-20852	Windows Hello 改ざんの脆弱性	重要	7.7	No	No	改ざん
69	CVE-2026-20929	Windows HTTP.sys 特権昇格の脆弱性	重要	7.5	No	No	特権昇格
70	CVE-2026-20825	Windows Hyper-V 情報漏洩脆弱性	重要	4.4	No	No	情報漏洩
71	CVE-2026-20816	Windows インストーラー 特権昇格脆弱性	重要	7.8	No	No	特権昇格
72	CVE-2026-20849	Windows Kerberos 特権昇格脆弱性	重要	7.5	No	No	特権昇格
73	CVE-2026-20833 †	Windows Kerberos 情報漏洩脆弱性	重要	5.5	No	No	情報漏洩
74	CVE-2026-20818	Windows カーネル情報漏洩脆弱性	重要	6.2	No	No	情報漏洩
75	CVE-2026-20838	Windows カーネル情報漏洩脆弱性	重要	5.5	No	No	情報漏洩
76	CVE-2026-20809	Windows カーネルメモリ特権昇格脆弱性	重要	7.8	No	No	特権昇格
77	CVE-2026-20859	Windows カーネルモード ドライバー特権昇格脆弱性	重要	7.8	No	No	特権昇格
78	CVE-2026-20875	Windows ローカルセキュリティ 機関サブシステムサービス (LSASS) サービス拒否脆弱性	重要	7.5	No	No	DoS攻撃
79	CVE-2026-20869	Windows ローカルセッションマネージャー (LSM) 特権昇格脆弱性	重要	7	No	No	特権昇格
80	CVE-2026-20858	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
81	CVE-2026-20861	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
82	CVE-2026-20865	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
83	CVE-2026-20866	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
84	CVE-2026-20867	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
85	CVE-2026-20873	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
86	CVE-2026-20874	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
87	CVE-2026-20877	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
88	CVE-2026-20918	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
89	CVE-2026-20923	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格

90	CVE-2026-20924	Windows Management Services 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
91	CVE-2026-20862	Windows Management Services 情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
92	CVE-2026-20837	Windows Media 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
93	CVE-2026-20936	Windows NDIS 情報漏洩の脆弱性	重要	4.3	No	No	情報漏洩
94	CVE-2026-20840	Windows NTFS 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
95	CVE-2026-20922	Windows NTFS 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
96	CVE-2026-20824	Windows リモートアシスタンスのセキュリティ機能バイパスの脆弱性	重要	5.5	No	No	セキュリティ機能バイパス
97	CVE-2026-20832	Windows リモートプロシージャコール インターフェイス定義言語 (IDL) の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
98	CVE-2026-20828	Windows rndismp6.sys 情報漏洩の脆弱性	重要	4.6	No	No	情報漏洩
99	CVE-2026-20843	Windows ルーティングおよびリモートアクセス サービス (RRAS) の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
100	CVE-2026-20868	Windows ルーティングおよびリモートアクセス サービス (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
101	CVE-2026-20856	Windows Server Update Service (WSUS) 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
102	CVE-2026-20927	Windows SMB サーバー サービス拒否の脆弱性	重要	5.3	No	No	DoS攻撃
103	CVE-2026-20848	Windows SMB サーバー 特権昇格の脆弱性	重要	7.5	No	No	特権昇格
104	CVE-2026-20919	Windows SMB サーバー 特権昇格の脆弱性	重要	7.5	No	No	特権昇格
105	CVE-2026-20921	Windows SMB サーバー 特権昇格の脆弱性	重要	7.5	No	No	特権昇格
106	CVE-2026-20926	Windows SMB サーバー特権昇格の脆弱性	重要	7.5	No	No	特権昇格
107	CVE-2026-20934	Windows SMB サーバー特権昇格の脆弱性	重要	7.5	No	No	特権昇格
108	CVE-2026-20834	Windows スプーフィングの脆弱性	重要	4.6	No	No	なりすまし
109	CVE-2026-20931	Windows 電話サービス特権昇格の脆弱性	重要	8	No	No	特権昇格
110	CVE-2026-20938	Windows 仮想化ベースのセキュリティ (VBS) エンクレープ特権昇格の脆弱性	重要	7.8	No	No	特権昇格
111	CVE-2026-20819	Windows 仮想化ベースのセキュリティ (VBS) 情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
112	CVE-2026-20935	Windows 仮想化ベースのセキュリティ (VBS) 情報漏洩の脆弱性	重要	6.2	No	No	情報漏洩
113	CVE-2026-20853	Windows WalletService 特権昇格の脆弱性	重要	7.4	No	No	特権昇格
114	CVE-2026-20870	Windows Win32 カーネルサブシステム 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
115	CVE-2026-0628 *	Chromium: CVE-2026-0628 WebView タグにおけるポリシー適用不足	高	N/A	No	No	セキュリティ機能バイパス

*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。