2022 年 9 月に Microsoft が発表した CVE の全リスト

*の印の CVE は、以前はサードパーティの製品であり、現在は Microsoft 製品に組み込まれていることを示しています。

	CVE 番号	タイトル	深刻度	CVSS	周知済か	悪用されたか	脆弱性タイプ
1	CVE-2022-37969	Windows 共通ログファイルシステムドライバに特権昇格の脆弱性	重要	7.8	Yes	Yes	特権昇格
2	CVE-2022-23960 *	Arm: CVE-2022-23960 キャッシュ投機制限の脆弱性	重要	N/A	Yes	No	情報漏えい
3	CVE-2022-34700	Microsoft Dynamics 365 (オンプレミス) の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
4	CVE-2022-35805	Microsoft Dynamics 365 (オンプレミス) の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-2022-34721	Windows Internet Key Exchange (IKE) Protocol Extensions のリモートコード実行の脆弱性	緊急	9.8	No	No	リモートコード実行
6	CVE-2022-34722	Windows Internet Key Exchange (IKE) Protocol Extensions のリモートコード実行の脆弱性	緊急	9.8	No	No	リモートコード実行
7	CVE-2022-34718	Windows TCP/IP リモートコード実行の脆弱性	緊急	9.8	No	No	リモートコード実行
8	CVE-2022-38013	.NET Core と Visual Studio のサービス拒否の脆弱性	重要	7.5	No	No	DoS 攻撃
9	CVE-2022-26929	.NET Framework の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
10	CVE-2022-38019	AV1 Video Extension の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
11	CVE-2022-38007	Azure Guest Configuration および Azure Arc 対応サーバーにおける特権昇格の脆弱性	重要	7.8	No	No	特権昇格

12	CVE-2022-37954	DirectX Graphics Kernel における特権昇格の脆弱性	重要	7.8	No	No	特権昇格
13	CVE-2022-35838	HTTP V3 Denial of Service の脆弱性	重要	7.5	No	No	DoS 攻撃
14	CVE-2022-35828	Microsoft Defender for Endpoint for Mac の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
15	CVE-2022-34726	Microsoft ODBC ドライバの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
16	CVE-2022-34727	Microsoft ODBC ドライバの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
17	CVE-2022-34730	Microsoft ODBC ドライバの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
18	CVE-2022-34732	Microsoft ODBC ドライバの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-2022-34734	Microsoft ODBC ドライバの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
20	CVE-2022-37963	Microsoft Office Visio の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
21	CVE-2022-38010	Microsoft Office Visio の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
22	CVE-2022-34731	Microsoft OLE DB Provider for SQL Server の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
23	CVE-2022-34733	Microsoft OLE DB Provider for SQL Server の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
24	CVE-2022-35834	Microsoft OLE DB Provider for SQL Server の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
25	CVE-2022-35835	Microsoft OLE DB Provider for SQL Server の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-2022-35836	Microsoft OLE DB Provider for SQL Server の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-2022-35840	Microsoft OLE DB Provider for SQL Server の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
28	CVE-2022-37962	Microsoft PowerPoint の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
29	CVE-2022-35823	Microsoft SharePoint の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
30	CVE-2022-37961	Microsoft SharePoint Server Remote Code Execution Vulnerability	重要	8.8	No	No	リモートコード実行
31	CVE-2022-38008	Microsoft SharePoint Server Remote Code Execution Vulnerability	重要	8.8	No	No	リモートコード実行
32	CVE-2022-38009	Microsoft SharePoint Server Remote Code Execution Vulnerability	重要	8.8	No	No	リモートコード実行
33	CVE-2022-37959	Network Device Enrollment Service (NDES) のセキュリティ機能回避の脆弱性	重要	6.5	No	No	セキュリティ機能バイパス
34	CVE-2022-38011	Raw Image Extension 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
35	CVE-2022-35830	リモートプロシージャコール実行時の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
36	CVE-2022-37958	SPNEGO Extended Negotiation (NEGOEX) セキュリティ機構に関する情報漏えいの脆弱性	重要	7.5	No	No	情報漏えい
37	CVE-2022-38020	Visual Studio Code の特権昇格の脆弱性	重要	7.3	No	No	特権昇格
38	CVE-2022-34725	Windows ALPC の特権昇格の脆弱性	重要	7	No	No	特権昇格
39	CVE-2022-35803	Windows 共通ログファイルシステムドライバに特権昇格の脆弱性	重要	7.8	No	No	特権昇格

40	CVE-2022-30170	Windows Credential Roaming Service の特権昇格の脆弱性	重要	7.3	No	No	特権昇格
41	CVE-2022-34719	Windows 分散ファイルシステム（DFS）の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
42	CVE-2022-34724	Windows DNS サーバのサービス拒否の脆弱性	重要	7.5	No	No	DoS 攻撃
43	CVE-2022-34723	Windows DPAPI (Data Protection Application Programming Interface) 情報漏えいの脆弱性	重要	5.5	No	No	情報漏えい
44	CVE-2022-35841	Windows Enterprise App Management Service の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
45	CVE-2022-35832	Windows イベントトレースのサービス拒否の脆弱性	重要	5.5	No	No	DoS 攻撃
46	CVE-2022-38004	Windows Fax Service の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
47	CVE-2022-34729	Windows GDI 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
48	CVE-2022-38006	Windows グラフィックス・コンポーネントの情報漏洩の脆弱性	重要	6.5	No	No	情報漏えい
49	CVE-2022-34728	Windows グラフィックス・コンポーネントの情報漏洩の脆弱性	重要	5.5	No	No	情報漏えい
50	CVE-2022-35837	Windows グラフィックス・コンポーネントの情報漏洩の脆弱性	重要	5	No	No	情報漏えい
51	CVE-2022-37955	Windows グループポリシーの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
52	CVE-2022-34720	Windows の Internet Key Exchange (IKE) Extension のサービス拒否の脆弱性	重要	7.5	No	No	DoS 攻撃
53	CVE-2022-33647	Windows Kerberos の特権昇格の脆弱性	重要	8.1	No	No	特権昇格

54	CVE-2022-33679	Windows Kerberos の特権昇格の脆弱性	重要	8.1	No	No	特権昇格
55	CVE-2022-37956	Windows カーネルの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
56	CVE-2022-37957	Windows カーネルの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
57	CVE-2022-37964	Windows カーネルの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
58	CVE-2022-30200	Windows Lightweight Directory Access Protocol (LDAP)の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
59	CVE-2022-26928	Windows フォトインポート API の特権昇格の脆弱性	重要	7	No	No	特権昇格
60	CVE-2022-38005	Windows Print Spooler の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
61	CVE-2022-35831	Windows リモートアクセス接続マネージャの情報漏えいの脆弱性	重要	5.5	No	No	情報漏えい
62	CVE-2022-30196	Windows Secure Channel のサービス拒否の脆弱性	重要	8.2	No	No	DoS 攻撃
63	CVE-2022-35833	Windows Secure Channel のサービス拒否の脆弱性	重要	7.5	No	No	DoS 攻撃
64	CVE-2022-38012	Microsoft Edge (Chromium ベース) のリモートコード実行の脆弱性	低	7.7	No	No	リモートコード実行
65	CVE-2022-3038 *	Chromium：CVE-2022-3038 ネットワークサービスにおける Use After Free の脆弱性	緊急	N/A	No	No	リモートコード実行
66	CVE-2022-3075 *	Chromium：CVE-2022-3075 Mojo における不十分なデータ検証の脆弱性	高	N/A	No	Yes	リモートコード実行
67	CVE-2022-3039 *	Chromium：CVE-2022-3039 WebSQL における Use after free の不具合の脆弱性	高	N/A	No	No	リモートコード実行

68	CVE-2022-3040 *	Chromium：CVE-2022-3040 Layout における Use After Free の脆弱性	高	N/A	No	No	リモートコード実行
69	CVE-2022-3041 *	Chromium：CVE-2022-3041 WebSQL における Use after free の不具合の脆弱性	高	N/A	No	No	リモートコード実行
70	CVE-2022-3044 *	Chromium：CVE-2022-3044 Site Isolation における不適切な実装の脆弱性	高	N/A	No	No	N/A
71	CVE-2022-3045 *	Chromium：CVE-2022-3045 V8 における信頼されない入力の不十分な検証の脆弱性	高	N/A	No	No	リモートコード実行
72	CVE-2022-3046 *	Chromium：CVE-2022-3046 ブラウザのタグにおける Use After Free の脆弱性	高	N/A	No	No	リモートコード実行
73	CVE-2022-3047 *	Chromium：CVE-2022-3047 拡張機能 API における不十分なポリシー適用の脆弱性	中	N/A	No	No	セキュリティ機能バイパス
74	CVE-2022-3053 *	Chromium：CVE-2022-3053 Pointer Lock における不適切な実装の脆弱性	中	N/A	No	No	N/A
75	CVE-2022-3054 *	Chromium：CVE-2022-3054 DevTools における不十分なポリシー適用の脆弱性	中	N/A	No	No	セキュリティ機能バイパス
76	CVE-2022-3055 *	Chromium：CVE-2022-3055 パスワードにおける Use After Free の脆弱性	中	N/A	No	No	リモートコード実行
77	CVE-2022-3056 *	Chromium：CVE-2022-3056 コンテンツセキュリティポリシーにおける不十分なポリシー適用の脆弱性	低	N/A	No	No	セキュリティ機能バイパス
78	CVE-2022-3057 *	Chromium：CVE-2022-3057 iframe の不適切な実装 Sandbox の脆弱性	低	N/A	No	No	特権昇格
79	CVE-2022-3058 *	Chromium CVE-2022-3058 Sign-In Flow における Use After Free の脆弱性	低	N/A	No	No	リモートコード実行