2022 年 1 月の Microsoft 更新プログラムで対処している脆弱性一覧

CVE 識別番号	脆弱性名称	深刻度	CVSS	一般に公開	悪用	種類
CVE-2021-22947 *	オープン ソース Curl のリモートでコードが実行される脆弱性	緊急	N/A	あり	なし	RCE
CVE-2021-36976 *	Libarchive のリモートでコードが実行される脆弱性	重要	N/A	あり	なし	RCE
CVE-2022-21836	Windows 証明書のなりすましの脆弱性	重要	7.8	あり	なし	Spoofing
CVE-2022-21839	Windows イベント トレーシングの随意アクセス制御リストのサービス拒否の脆弱性	重要	6.1	あり	なし	DoS
CVE-2022-21874	Windows Security Center API のリモートでコードが実行される脆弱性	重要	7.8	あり	なし	RCE
CVE-2022-21919	Windows User Profile Service の特権の昇格の脆弱性	重要	7	あり	なし	EoP
CVE-2022-21857	Active Directory Domain Services の特権の昇格の脆弱性	緊急	8.8	なし	なし	EoP
CVE-2022-21912	DirectX Graphics カーネルのリモートでコードが実行される脆弱性	緊急	7.8	なし	なし	RCE
CVE-2022-21898	DirectX Graphics カーネルのリモートでコードが実行される脆弱性	緊急	7.8	なし	なし	RCE
CVE-2022-21917	HEVC ビデオ拡張機能のリモートでコードが実行される脆弱性	緊急	7.8	なし	なし	RCE
CVE-2022-21907	HTTP プロトコル スタックのリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	RCE
CVE-2022-21846	Microsoft Exchange Server のリモートでコードが実行される脆弱性	緊急	9	なし	なし	RCE

CVE-2022-21840	Microsoft Office のリモート コードが実行される脆弱性	緊急	8.8	なし	なし	RCE
CVE-2022-21833	仮想マシンの IDE ドライブの特権の昇格の脆弱性	緊急	7.8	なし	なし	EoP
CVE-2022-21911	.NET Framework のサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-21869	クリップボード ユーザー サービスの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21865	DirectX グラフィック カーネル ファイルのサービス拒否の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21918	DirectX グラフィック カーネル ファイルのサービス拒否の脆弱性	重要	6.5	なし	なし	DoS
CVE-2022-21913	ローカル セキュリティ機関 (ドメイン ポリシー) リモート プロトコルのセキュリティ機能のバイパス	重要	5.3	なし	なし	SFB
CVE-2022-21884	ローカル セキュリティ機関サブシステム サービスの特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21910	Microsoft クラスター ポート ドライバーの特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21835	Microsoft Cryptographic Services の特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21871	Microsoft 診断ハブ標準コレクター ランタイムの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21891	Microsoft Dynamics 365 Sales のなりすましの脆弱性	重要	7.6	なし	なし	Spoofing
CVE-2022-21932	Microsoft Dynamics 365 Customer Engagement のクロスサイト スクリプトの脆弱性	重要	7.6	なし	なし	XSS

CVE-2022-21970	Microsoft Edge (Chromium ベース) の特権の昇格の脆弱性	重要	6.1	なし	なし	EoP
CVE-2022-21841	Microsoft Excel のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-21855	Microsoft Exchange Server のリモートでコードが実行される脆弱性	重要	9	なし	なし	RCE
CVE-2022-21969	Microsoft Exchange Server のリモートでコードが実行される脆弱性	重要	9	なし	なし	RCE
CVE-2022-21837	Microsoft SharePoint Server のリモートでコードが実行される脆弱性	重要	8.3	なし	なし	RCE
CVE-2022-21842	Microsoft Word のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-21850	リモート デスクトップ クライアントのリモートでコードが実行される脆弱性	重要	8.8	なし	なし	RCE
CVE-2022-21851	リモート デスクトップ クライアントのリモートでコードが実行される脆弱性	重要	8.8	なし	なし	RCE
CVE-2022-21964	リモート デスクトップ ライセンス診断の情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-21893	リモート デスクトップ プロトコルのリモートでコードが実行される脆弱性	重要	8.8	なし	なし	RCE
CVE-2022-21922	リモート プロシージャ コール ランタイムのリモートでコードが実行される脆弱性	重要	8.8	なし	なし	RCE
CVE-2022-21894	セキュア ブートのセキュリティ機能のバイパスの脆弱性	重要	4.4	なし	なし	SFB
CVE-2022-21877	Storage Spaces Controller の情報漏えいの脆弱性	重要	5.5	なし	なし	Info

CVE-2022-21870	タブレット Windows ユーザー インターフェイス アプリケーション コアの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21861	タスク フロー データ エンジンの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21873	タイル データ リポジトリの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21882	Win32k の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21887	Win32k の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21876	Win32k の情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-21859	Windows Accounts Control の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21860	Windows AppContracts API Server の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21862	Windows Application Model Core API の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21925	Windows BackupKey リモート プロトコルのセキュリティ機能のバイパスの脆弱性	重要	5.3	なし	なし	SFB
CVE-2022-21858	Windows Bind Filter ドライバーの特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21838	Windows クリーンアップ マネージャーの特権の昇格の脆弱性	重要	5.5	なし	なし	EoP
CVE-2022-21916	Windows 共通ログ ファイル システム ドライバーの特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21897	Windows 共通ログ ファイル システム ドライバーの特権の昇格の脆弱性	重要	7.8	なし	なし	EoP

CVE-2022-21906	Windows Defender アプリケーション制御のセキュリティ機能のバイパスの脆弱性	重要	5.5	なし	なし	SFB
CVE-2022-21921	Windows Defender Credential Guard のセキュリティ機能のバイパスの脆弱性	重要	4.4	なし	なし	SFB
CVE-2022-21868	Windows Devices Human Interface の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21852	Windows DWM Core ライブラリの特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21902	Windows DWM Core ライブラリの特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21896	Windows DWM Core ライブラリの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21872	Windows Event Tracing の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21899	Windows Extensible Firmware Interface のセキュリティ機能のバイパスの脆弱性	重要	5.5	なし	なし	SFB
CVE-2022-21903	Windows GDI の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21904	Windows GDI の情報漏えいの脆弱性	重要	7.5	なし	なし	Info
CVE-2022-21915	Windows GDI+ の情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-21880	Windows GDI+ の情報漏えいの脆弱性	重要	7.5	なし	なし	Info
CVE-2022-21878	Windows Geolocation Service のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-21847	Windows Hyper-V のサービス拒否の脆弱性	重要	6.5	なし	なし	DoS

CVE-2022-21901	Windows Hyper-V の特権の昇格の脆弱性	重要	9	なし	なし	EoP
CVE-2022-21900	Windows Hyper-V のセキュリティ機能のバイパスの脆弱性	重要	4.6	なし	なし	SFB
CVE-2022-21905	Windows Hyper-V のセキュリティ機能のバイパスの脆弱性	重要	4.6	なし	なし	SFB
CVE-2022-21843	Windows IKE Extension のサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-21883	Windows IKE Extension のサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-21848	Windows IKE Extension のサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-21889	Windows IKE Extension のサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-21890	Windows IKE Extension のサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-21849	Windows IKE Extension のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	RCE
CVE-2022-21908	Windows インストーラーの特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21920	Windows Kerberos の特権の昇格の脆弱性	重要	8.8	なし	なし	EoP
CVE-2022-21879	Windows カーネルの特権の昇格の脆弱性	重要	5.5	なし	なし	EoP
CVE-2022-21881	Windows カーネルの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21888	Windows モダン実行サーバーのリモートでコードが実行される脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-21867	Windows プッシュ通知アプリの特権の昇格の脆弱性	重要	7	なし	なし	EoP

CVE-2022-21885	Windows Remote Access Connection Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21914	Windows Remote Access Connection Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21892	Windows Resilient File System (ReFS) のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	RCE
CVE-2022-21958	Windows Resilient File System (ReFS) のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	RCE
CVE-2022-21959	Windows Resilient File System (ReFS) のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	RCE
CVE-2022-21960	Windows Resilient File System (ReFS) のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	RCE
CVE-2022-21961	Windows Resilient File System (ReFS) のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	RCE
CVE-2022-21962	Windows Resilient File System (ReFS) のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	RCE
CVE-2022-21963	Windows Resilient File System (ReFS) のリモートでコードが実行される脆弱性	重要	6.4	なし	なし	RCE
CVE-2022-21928	Windows Resilient File System (ReFS) のリモートでコードが実行される脆弱性	重要	6.3	なし	なし	RCE
CVE-2022-21863	Windows StateRepository API Server ファイルの特権の昇格の脆弱性	重要	7	なし	なし	RCE

CVE-2022-21875	Windows ストレージの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21866	Windows System Launcher の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21864	Windows UI Immersive Server API の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21895	Windows UI Immersive Server API の特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-21834	Windows ユーザー モード ドライバー フレームワーク リフレクター ドライバーの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-21924	ワークステーション サービス リモート プロトコルのセキュリティ機能のバイパスの脆弱性	重要	5.3	なし	なし	SFB
CVE-2022-0096 *	Chromium: CVE-2022-0096 Use after free in Storage	緊急	N/A	なし	なし	
CVE-2022-0097 *	Chromium: CVE-2022-0097 Inappropriate implementation in DevTools	高	N/A	なし	なし	
CVE-2022-0098 *	Chromium: CVE-2022-0098 Use after free in Screen Capture	高	N/A	なし	なし	
CVE-2022-0099 *	Chromium: CVE-2022-0099 Use after free in Sign-in	高	N/A	なし	なし	
CVE-2022-0100 *	Chromium: CVE-2022-0100 Heap buffer overflow in Media streams API	高	N/A	なし	なし	
CVE-2022-0101 *	Chromium: CVE-2022-0101 Heap buffer overflow in Bookmarks	高	N/A	なし	なし	
CVE-2022-0102 *	Chromium: CVE-2022-0102 Type Confusion in V8	高	N/A	なし	なし	
CVE-2022-0103 *	Chromium: CVE-2022-0103 Use after free in SwiftShader	高	N/A	なし	なし	

CVE-2022-0104 *	Chromium: CVE-2022-0104 Heap buffer overflow in ANGLE	高	N/A	なし	なし	
CVE-2022-0105 *	Chromium: CVE-2022-0105 Use after free in PDF	高	N/A	なし	なし	
CVE-2022-0106 *	Chromium: CVE-2022-0106 Use after free in Autofill	高	N/A	なし	なし	
CVE-2022-0107 *	Chromium: CVE-2022-0107 Use after free in File Manager API	中	N/A	なし	なし	
CVE-2022-0108 *	Chromium: CVE-2022-0108 Inappropriate implementation in Navigation	中	N/A	なし	なし	
CVE-2022-0109 *	Chromium: CVE-2022-0109 Inappropriate implementation in Autofill	中	N/A	なし	なし	
CVE-2022-0110 *	Chromium: CVE-2022-0110 Incorrect security UI in Autofill	中	N/A	なし	なし	
CVE-2022-0111 *	Chromium: CVE-2022-0111 Inappropriate implementation in Navigation	中	N/A	なし	なし	
CVE-2022-0112 *	Chromium: CVE-2022-0112 Incorrect security UI in Browser UI	中	N/A	なし	なし	
CVE-2022-0113 *	Chromium: CVE-2022-0113 Inappropriate implementation in Blink	中	N/A	なし	なし	
CVE-2022-0114 *	Chromium: CVE-2022-0114 Out of bounds memory access in Web Serial	中	N/A	なし	なし	
CVE-2022-0115 *	Chromium: CVE-2022-0115 Uninitialized Use in File API	中	N/A	なし	なし	
CVE-2022-0116 *	Chromium: CVE-2022-0116 Inappropriate implementation in Compositing	中	N/A	なし	なし	

CVE-2022-0117 *	Chromium: CVE-2022-0117 Policy bypass in Service Workers	低	N/A	なし	なし	
CVE-2022-0118 *	Chromium: CVE-2022-0118 Inappropriate implementation in WebShare	低	N/A	なし	なし	
CVE-2022-0120 *	Chromium: CVE-2022-0120 Inappropriate implementation in Passwords	低	N/A	なし	なし	

*この脆弱性は過去にサードパーティによって公開済みであり、現在では Microsoft 製品に組み込まれていることを示します。