2022 年 4 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 スコア	一般公開	悪用の事実	種類
CVE-2022-24521	Windows 共通ログ ファイル システム ドライバにおける特権昇格の脆弱性	重要	7.8	なし	あり	EoP
CVE-2022-26904	Windows User Profile Service における特権昇格の脆弱性	重要	7	あり	なし	EoP
CVE-2022-23259	Microsoft Dynamics 365 (オンプレミス) におけるリモートコード実行の脆弱性	緊急	8.8	なし	なし	RCE
CVE-2022-26809	リモート プロシージャ コール ランタイムにおけるリモートコード実行の脆弱性	緊急	9.8	なし	なし	RCE
CVE-2022-22008	Windows Hyper-V におけるリモートコード実行の脆弱性	緊急	7.7	なし	なし	RCE
CVE-2022-23257	Windows Hyper-V におけるリモートコード実行の脆弱性	緊急	8.6	なし	なし	RCE
CVE-2022-24537	Windows Hyper-V におけるリモートコード実行の脆弱性	緊急	7.7	なし	なし	RCE
CVE-2022-26919	Windows LDAP におけるリモートコード実行の脆弱性	緊急	8.1	なし	なし	RCE
CVE-2022-24491	Microsoft ネットワーク ファイル システムにおけるリモートコード実行の脆弱性	緊急	9.8	なし	なし	RCE

CVE-2022-24497	Microsoft ネットワーク ファイル システムにおけるリモートコード実行の脆弱性	緊急	9.8	なし	なし	RCE
CVE-2022-24541	Windows Server Service におけるリモートコード実行の脆弱性	緊急	8.8	なし	なし	RCE
CVE-2022-24500	Windows SMB におけるリモートコード実行の脆弱性	緊急	8.8	なし	なし	RCE
CVE-2022-26832	.NET Framework におけるサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-26907	Azure SDK for .NET における情報漏えいの脆弱性	重要	5.3	なし	なし	Info
CVE-2022-26896	Azure Site Recovery における特権昇格の脆弱性	重要	4.9	なし	なし	EoP
CVE-2022-26897	Azure Site Recovery における特権昇格の脆弱性	重要	4.9	なし	なし	EoP
CVE-2022-26898	Azure Site Recovery におけるリモートコード実行の脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-24489	Cluster Client Failover (CCF) における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24479	接続ユーザー エクスペリエンスとテレメトリにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26830	DiskUsage.exe におけるリモートコード実行の脆弱性	重要	7.5	なし	なし	RCE
CVE-2022-24767	GitHub: SYSTEM ユーザ アカウントで Git for Windows のアンインストーラを実行した	重要	記載なし	なし	なし	EoP

	場合における DLL ハイジャックの脆弱性					
CVE-2022-24765	GitHub: Git for Windows での Git ディレクトリの制御されていない検索	重要	記載なし	なし	なし	EoP
CVE-2022-24532	HEVC ビデオ拡張機能におけるリモートコード実行の脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-24496	ローカル セキュリティ機関 (LSA) における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24548	Microsoft Defender におけるサービス拒否の脆弱性	重要	5.5	なし	なし	DoS
CVE-2022-24475	Microsoft Edge (Chromium ベース) における特権昇格の脆弱性	重要	8.3	なし	なし	EoP
CVE-2022-26891	Microsoft Edge (Chromium ベース) における特権昇格の脆弱性	重要	8.3	なし	なし	EoP
CVE-2022-26894	Microsoft Edge (Chromium ベース) における特権昇格の脆弱性	重要	8.3	なし	なし	EoP
CVE-2022-26895	Microsoft Edge (Chromium ベース) における特権昇格の脆弱性	重要	8.3	なし	なし	EoP
CVE-2022-26900	Microsoft Edge (Chromium ベース) における特権昇格の脆弱性	重要	8.3	なし	なし	EoP

CVE-2022-26908	Microsoft Edge (Chromium ベース) における特権昇格の脆弱性	重要	8.3	なし	なし	EoP
CVE-2022-24473	Microsoft Excel におけるリモートコード実行の脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-26901	Microsoft Excel におけるリモートコード実行の脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-26924	YARP におけるサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-24493	Microsoft Local Security Authority (LSA) Server における情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-23292	Microsoft Power BI におけるなりすましの脆弱性	重要	7.1	なし	なし	Spoofing
CVE-2022-24472	Microsoft SharePoint Server におけるなりすましの脆弱性	重要	8	なし	なし	Spoofing
CVE-2022-26788	PowerShell における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24533	リモート デスクトップ プロトコルにおけるリモートコード実行の脆弱性	重要	8	なし	なし	RCE
CVE-2022-24492	リモート プロシージャ コール ランタイムにおけるリモートコード実行の脆弱性	重要	8.8	なし	なし	RCE
CVE-2022-24528	リモート プロシージャ コール ランタイムにおけるリモートコード実行の脆弱性	重要	8.8	なし	なし	RCE
CVE-2022-26910	Skype for Business と Lync におけるなりすましの脆弱性	重要	5.3	なし	なし	Spoofing

CVE-2022-26911	Skype for Business における情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-26921	Visual Studio Code における特権昇格の脆弱性	重要	記載なし	なし	なし	EoP
CVE-2022-24513	Visual Studio における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24485	Win32 File Enumeration におけるリモートコード実行の脆弱性	重要	7.5	なし	なし	RCE
CVE-2022-21983	Win32 Stream Enumeration におけるリモートコード実行の脆弱性	重要	7.5	なし	なし	RCE
CVE-2022-24534	Win32 Stream Enumeration におけるリモートコード実行の脆弱性	重要	7.5	なし	なし	RCE
CVE-2022-26914	Win32k における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24482	Windows ALPC における特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-24540	Windows ALPC における特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-24494	WinSock 用 Windows Ancillary Function Driver における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24549	Windows AppX パッケージ マネージャーにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26828	Windows Bluetooth ドライバにおける特権昇格の脆弱性	重要	7	なし	なし	EoP

CVE-2022-24484	Windows クラスター共有ボリューム (CSV) におけるサービス拒否の脆弱性	重要	5.5	なし	なし	DoS
CVE-2022-24538	Windows クラスター共有ボリューム (CSV) におけるサービス拒否の脆弱性	重要	6.5	なし	なし	DoS
CVE-2022-26784	Windows クラスター共有ボリューム (CSV) におけるサービス拒否の脆弱性	重要	6.5	なし	なし	DoS
CVE-2022-24481	Windows 共通ログ ファイル システム ドライバにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24488	Windows デスクトップ ブリッジにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24547	Windows Digital Media Receiver における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24495	Windows Direct Show - リモートコード実行の脆弱性	重要	7	なし	なし	RCE
CVE-2022-26816	Windows DNS サーバにおける情報漏えいの脆弱性	重要	4.9	なし	なし	Info
CVE-2022-24536	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-26811	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.2	なし	なし	RCE

CVE-2022-26812	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	6.7	なし	なし	RCE
CVE-2022-26813	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-26814	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.5	なし	なし	RCE
CVE-2022-26815	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	8.8	なし	なし	RCE
CVE-2022-26817	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.5	なし	なし	RCE
CVE-2022-26818	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.5	なし	なし	RCE
CVE-2022-26819	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	6.6	なし	なし	RCE
CVE-2022-26820	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	6.6	なし	なし	RCE
CVE-2022-26821	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	6.6	なし	なし	RCE
CVE-2022-26822	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	6.6	なし	なし	RCE

CVE-2022-26823	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-26824	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-26825	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-26826	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-26829	Windows DNS サーバにおけるリモートコード実行の脆弱性	重要	7.5	なし	なし	RCE
CVE-2022-24546	Windows DWM Core ライブラリにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24527	Windows Endpoint Configuration Manager における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26916	Windows Fax Compose Form におけるリモートコード実行の脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-26917	Windows Fax Compose Form におけるリモートコード実行の脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-26918	Windows Fax Compose Form におけるリモートコード実行の脆弱性	重要	7.8	なし	なし	RCE

CVE-2022-26808	Windows エクスプローラにおける特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-26810	Windows File Server Resource Management Service における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26827	Windows File Server Resource Management Service における特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-26920	Windows Graphics コンポーネントにおける情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-26903	Windows グラフィックス コンポーネントにおけるリモートコード実行の脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-23268	Windows Hyper-V におけるサービス拒否の脆弱性	重要	6.5	なし	なし	DoS
CVE-2022-22009	Windows Hyper-V におけるリモートコード実行の脆弱性	重要	7.7	なし	なし	RCE
CVE-2022-24490	Windows Hyper-V 共有仮想ハード ディスクにおける情報漏えいの脆弱性	重要	8.1	なし	なし	Info
CVE-2022-24539	Windows Hyper-V 共有仮想ハード ディスクにおける情報漏えいの脆弱性	重要	8.1	なし	なし	Info
CVE-2022-26783	Windows Hyper-V 共有仮想ハード ディスクにおける情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-26785	Windows Hyper-V 共有仮想ハード ディスクにおける情報漏えいの脆弱性	重要	6.5	なし	なし	Info

CVE-2022-24499	Windows インストーラーにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24530	Windows インストーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24498	Windows iSCSI Target サービスにおける情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-24486	Windows Kerberos における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24544	Windows Kerberos における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24545	Windows Kerberos におけるリモートコード実行の脆弱性	重要	8.1	なし	なし	RCE
CVE-2022-24483	Windows カーネルにおける情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-26831	Windows カーネルにおける情報漏えいの脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-24487	Windows ローカル セキュリティ機関 (LSA) におけるリモートコード実行の脆弱性	重要	8.8	なし	なし	RCE
CVE-2022-26786	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26787	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26789	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26790	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP

CVE-2022-26791	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26792	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26793	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26794	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26795	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26796	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26797	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26798	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26801	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26802	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26803	Windows 印刷スプーラにおける特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26915	Windows Secure Channel におけるサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-24550	Windows Telephony Server における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24543	Windows Upgrade Assistant におけるリモートコード実行の脆弱性	重要	7.8	なし	なし	RCE

CVE-2022-24474	Windows Win32k における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24542	Windows Win32k における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26807	Windows Work Folder Service における特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-26909	Microsoft Edge (Chromium ベース) における特権昇格の脆弱性	警告	8.3	なし	なし	EoP
CVE-2022-26912	Microsoft Edge (Chromium ベース) における特権昇格の脆弱性	警告	8.3	なし	なし	EoP
CVE-2022-24523	Microsoft Edge (Chromium ベース) におけるなりすましの脆弱性	警告	4.3	なし	なし	EoP
CVE-2022-1129 *	Chromium: Inappropriate implementation in Full Screen Mode	高	N/A	なし	なし	RCE
CVE-2022-1128 *	Chromium: Inappropriate implementation in Web Share API	高	N/A	なし	なし	RCE
CVE-2022-1130 *	Chromium: Insufficient validation of untrusted input in WebOTP	高	N/A	なし	なし	RCE
CVE-2022-1134 *	Chromium: Type Confusion in V8	高	N/A	なし	なし	RCE
CVE-2022-1232 *	Chromium: Type Confusion in V8	高	N/A	なし	なし	RCE
CVE-2022-1131 *	Chromium: Use after free in Cast UI	高	N/A	なし	なし	RCE
CVE-2022-1125 *	Chromium: Use after free in Portals	高	N/A	なし	なし	RCE

CVE-2022-1127 *	Chromium: Use after free in QR Code Generator	高	N/A	なし	なし	RCE
CVE-2022-1133 *	Chromium: Use after free in WebRTC	高	N/A	なし	なし	RCE
CVE-2022-1143 *	Chromium: Heap buffer overflow in WebUI	中	N/A	なし	なし	RCE
CVE-2022-1139 *	Chromium: Inappropriate implementation in Background Fetch API	中	N/A	なし	なし	N/A
CVE-2022-1137 *	Chromium: Inappropriate implementation in Extensions	中	N/A	なし	なし	N/A
CVE-2022-1138 *	Chromium: Inappropriate implementation in Web Cursor	中	N/A	なし	なし	N/A
CVE-2022-1145 *	Chromium: Use after free in Extensions	中	N/A	なし	なし	RCE
CVE-2022-1135 *	Chromium: Use after free in Shopping Cart	中	N/A	なし	なし	RCE
CVE-2022-1136 *	Chromium: Use after free in Tab Strip	中	N/A	なし	なし	RCE
CVE-2022-1146 *	Chromium: Inappropriate implementation in Resource Timing	低	N/A	なし	なし	EoP

*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 社製品に組み込まれていることを示します。

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thoughtprovoking research that can shape strategic industry direction. www.trendmicro.com