2022 年 3 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-2022-24512	.NET と Visual Studio のリモート コードが実行される脆弱性	重要	6.3	あり	なし	RCE
CVE-2022-21990	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	あり	なし	RCE
CVE-2022-24459	Windows Fax とスキャン サービスの特権の昇格の脆弱性	重要	7.8	あり	なし	EoP
CVE-2022-22006	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-2022-23277	Microsoft Exchange Server のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	RCE
CVE-2022-24501	VP9 Video 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-2022-24508	Windows SMBv3 クライアント/サーバー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-2022-21967	Xbox Live Auth Manager for Windows の特権の昇格の脆弱性	重要	7	なし	なし	EoP

CVE-2022-24464	.NET および Visual Studio のサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-24469	Azure Site Recovery の特権の昇格の脆弱性	重要	8.1	なし	なし	EoP
CVE-2022-24506	Azure Site Recovery の特権の昇格の脆弱性	重要	6.5	なし	なし	EoP
CVE-2022-24515	Azure Site Recovery の特権の昇格の脆弱性	重要	6.5	なし	なし	EoP
CVE-2022-24518	Azure Site Recovery の特権の昇格の脆弱性	重要	6.5	なし	なし	EoP
CVE-2022-24519	Azure Site Recovery の特権の昇格の脆弱性	重要	6.5	なし	なし	EoP
CVE-2022-24467	Azure Site Recovery のリモートでコードが実行される脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-24468	Azure Site Recovery のリモートでコードが実行される脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-24470	Azure Site Recovery のリモートでコードが実行される脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-24471	Azure Site Recovery のリモートでコードが実行される脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-24517	Azure Site Recovery のリモートでコードが実行される脆弱性	重要	7.2	なし	なし	RCE

CVE-2022-24520	Azure Site Recovery のリモートでコードが実行される脆弱性	重要	7.2	なし	なし	RCE
CVE-2020-8927 *	Brotli ライブラリのバッファー オーバーフローの脆弱性	重要	6.5	なし	なし	N/A
CVE-2022-24457	HEIF 画像拡張機能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-2022-22007	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	重要	7.8	なし	なし	RCE
CVE-2022-23301	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	重要	7.8	なし	なし	RCE
CVE-2022-24452	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	重要	7.8	なし	なし	RCE
CVE-2022-24453	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	重要	7.8	なし	なし	RCE
CVE-2022-24456	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	重要	7.8	なし	なし	RCE
CVE-2022-21977	メディア ファンデーションの情報漏えいの脆弱性	重要	3.3	なし	なし	Info
CVE-2022-22010	メディア ファンデーションの情報漏えいの脆弱性	重要	4.4	なし	なし	Info
CVE-2022-23278	Microsoft Defender for Endpoint のなりすましの脆弱性	重要	5.9	なし	なし	Spoofing

CVE-2022-23266	Microsoft Defender for IoT の特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-23265	Microsoft Defender for IoT のリモートでコードが実行される脆弱性	重要	7.2	なし	なし	RCE
CVE-2022-24463	Microsoft Exchange Server のなりすましの脆弱性	重要	6.5	なし	なし	Spoofing
CVE-2022-24465	IOS 用 Microsoft Intune ポータルのセキュリティ機能のバイパスの脆弱性	重要	3.3	なし	なし	SFB
CVE-2022-24461	Microsoft Office Visio 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-2022-24509	Microsoft Office Visio 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-2022-24510	Microsoft Office Visio 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-2022-24511	Microsoft Office Word の改ざんの脆弱性	重要	5.5	なし	なし	Tampering
CVE-2022-24462	Microsoft Word 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-2022-23282	ペイント 3D 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-2022-23253	Point-to-Point Tunneling プロトコルのサービス拒否の脆弱性	重要	6.5	なし	なし	DoS

CVE-2022-23295	Raw 画像拡張機能のリモードでコードが実行される脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-23300	Raw 画像拡張機能のリモードでコードが実行される脆弱性	重要	7.8	なし	なし	RCE
CVE-2022-23285	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-2022-24503	リモート デスクトップ プロトコル クライアントの情報漏えいの脆弱性	重要	5.4	なし	なし	Info
CVE-2022-24522	Chrome 用 Skype 拡張機能の情報漏えいの脆弱性	重要	7.5	なし	なし	Info
CVE-2022-24460	タブレット Windows ユーザー インターフェイス アプリケーションの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-24526	Visual Studio Code のなりすましの脆弱性	重要	6.1	なし	なし	Spoofing
CVE-2022-24451	VP9 Video 拡張機能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-2022-23283	Windows ALPC の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-23287	Windows ALPC の特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-24505	Windows ALPC の特権の昇格の脆弱性	重要	7	なし	なし	EoP

CVE-2022-24507	WinSock 用 Windows Ancillary Function Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-24455	Windows CD-ROM 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-2022-23286	Windows Cloud Files Mini Filter ドライバーの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-23281	Windows 共通ログ ファイル システム ドライバーの情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-23288	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-2022-23291	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-2022-23294	Windows イベント トレーシング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-2022-23293	Windows Fast FAT 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-2022-24502	Windows HTML プラットフォームのセキュリティ機能のバイパスの脆弱性	重要	4.3	なし	なし	SFB
CVE-2022-21975	Windows Hyper-V のサービス拒否の脆弱性	重要	4.7	なし	なし	DoS
CVE-2022-23290	Windows Inking COM の特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-23296	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-2022-21973	Windows Media Center 更新プログラムのサービス拒否の脆弱性	重要	5.5	なし	なし	DoS
CVE-2022-23297	Windows NT Lan Manager Datagram Receiver ドライバーの情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-23298	Windows NT OS カーネルの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-23299	Windows PDEV の特権の昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-23284	Windows 印刷スプーラーの特権の昇格の脆弱性	重要	7.2	なし	なし	EoP
CVE-2022-24454	Windows Security Support Provider Interface の特権の昇格の脆弱性 ity	重要	7.8	なし	なし	EoP
CVE-2022-24525	Windows Update スタックの特権の昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-0789 *	Chromium: Heap buffer overflow in ANGLE	高	N/A	なし	なし	RCE
CVE-2022-0797 *	Chromium: Out of bounds memory access in Mojo	高	N/A	なし	なし	RCE
CVE-2022-0792 *	Chromium: Out of bounds read in ANGLE	高	N/A	なし	なし	RCE
CVE-2022-0795 *	Chromium: Type Confusion in Blink Layout	高	N/A	なし	なし	RCE
CVE-2022-0790 *	Chromium: Use after free in Cast UI	高	N/A	なし	なし	RCE
CVE-2022-0796 *	Chromium: Use after free in Media	高	N/A	なし	なし	RCE
CVE-2022-0791 *	Chromium: Use after free in Omnibox	高	N/A	なし	なし	RCE

CVE-2022-0793 *	Chromium: Use after free in Views	高	N/A	なし	なし	RCE
CVE-2022-0794 *	Chromium: Use after free in WebShare	高	N/A	なし	なし	RCE
CVE-2022-0800 *	Chromium: Heap buffer overflow in Cast UI	中	N/A	なし	なし	RCE
CVE-2022-0807 *	Chromium: Inappropriate implementation in Autofill	中	N/A	なし	なし	Info
CVE-2022-0802 *	Chromium: Inappropriate implementation in Full screen mode	中	N/A	なし	なし	Info
CVE-2022-0804 *	Chromium: Inappropriate implementation in Full screen mode	中	N/A	なし	なし	Info
CVE-2022-0801 *	Chromium: Inappropriate implementation in HTML parser	中	N/A	なし	なし	Tampering
CVE-2022-0803 *	Chromium: Inappropriate implementation in Permissions	中	N/A	なし	なし	SFB
CVE-2022-0799 *	Chromium: Insufficient policy enforcement in Installer	中	N/A	なし	なし	SFB
CVE-2022-0809 *	Chromium: Out of bounds memory access in WebXR	中	N/A	なし	なし	RCE
CVE-2022-0805 *	Chromium: Use after free in Browser Switcher	中	N/A	なし	なし	RCE
CVE-2022-0808 *	Chromium: Use after free in Chrome OS Shell	中	N/A	なし	なし	RCE
CVE-2022-0798 *	Chromium: Use after free in MediaStream	中	N/A	なし	なし	RCE

*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