2022 年 5 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-2022-26925	Windows ローカルセキュリティ機関（LSA）におけるなりすましの脆弱性	重要	8.1	あり	あり	Spoofing
CVE-2022-29972	Insight Software: CVE-2022-29972 Magnitude Simba Amazon Redshift ODBC Driver	緊急	N/A	あり	なし	RCE
CVE-2022-22713	Windows Hyper-V におけるサービス拒否の脆弱性	重要	5.6	あり	なし	DoS
CVE-2022-26923	Active Directory ドメインサービスにおける特権昇格の脆弱性	緊急	8.8	なし	なし	EoP
CVE-2022-21972	Point-to-Point Tunneling プロトコル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-2022-23270	Point-to-Point Tunneling プロトコル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-2022-22017	リモート デスクトップ クライアント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-2022-26931	Windows Kerberos における特権昇格の脆弱性	緊急	7.5	なし	なし	EoP
CVE-2022-26937	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-2022-23267	.NET and Visual Studio におけるサービス拒否の脆弱性	重要	7.5	なし	なし	DoS

CVE-2022-29117	.NET and Visual Studio におけるサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-29145	.NET and Visual Studio におけるサービス拒否の脆弱性	重要	7.5	なし	なし	DoS
CVE-2022-29127	BitLocker におけるセキュリティ機能を回避される脆弱性	重要	4.2	なし	なし	SFB
CVE-2022-29109	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-2022-29110	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-2022-21978	Microsoft Exchange Server における特権昇格の脆弱性	重要	8.2	なし	なし	EoP
CVE-2022-29107	Microsoft Office におけるセキュリティ機能を回避される脆弱性	重要	5.5	なし	なし	SFB
CVE-2022-29108	Microsoft SharePoint Server 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-2022-29105	Microsoft Windows Media Foundation 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-2022-26940	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	6.5	なし	なし	Info
CVE-2022-22019	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-2022-26932	記憶域スペース ダイレクトにおける特権昇格の脆弱性	重要	8.2	なし	なし	EoP
CVE-2022-26938	記憶域スペース ダイレクトにおける特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-26939	記憶域スペース ダイレクトにおける特権昇格の脆弱性	重要	7	なし	なし	EoP

CVE-2022-29126	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 コアにおける特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-30129	Visual Studio Code 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-2022-29148	Visual Studio 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-2022-26926	Windows アドレス帳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-2022-23279	Windows ALPC における特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-26913	Windows 認証におけるセキュリティ機能を回避される脆弱性	重要	7.4	なし	なし	SFB
CVE-2022-29135	Windows クラスタ共有ボリューム（CSV）における特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-29150	Windows クラスタ共有ボリューム（CSV）における特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-29151	Windows クラスタ共有ボリューム（CSV）における特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-29138	Windows クラスタ共有ボリュームにおける特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-29120	Windows クラスタ共有ボリュームにおける情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-29122	Windows クラスタ共有ボリュームにおける情報漏えいの脆弱性	重要	6.5	なし	なし	Info

CVE-2022-29123	Windows クラスタ共有ボリュームにおける情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-29134	Windows クラスタ共有ボリュームにおける情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-29113	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-2022-29102	フェールオーバー クラスタにおける情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-29115	Windows Fax サービス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-2022-22011	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-2022-26934	Windows Graphics コンポーネントにおける情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-29112	Windows Graphics コンポーネントにおける情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-26927	Windows Graphics 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	8.8	なし	なし	RCE
CVE-2022-24466	Windows Hyper-V におけるセキュリティ機能を回避される脆弱性	重要	4.1	なし	なし	SFB
CVE-2022-29106	Windows Hyper-V 共有仮想ディスクにおける特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-29133	Windows カーネルにおける特権昇格の脆弱性	重要	8.8	なし	なし	EoP
CVE-2022-29142	Windows カーネルにおける特権昇格の脆弱性	重要	7	なし	なし	EoP

CVE-2022-29116	Windows カーネルにおける情報漏えいの脆弱性	重要	4.7	なし	なし	Info
CVE-2022-22012	Windows LDAP におけるリモートコード実行の脆弱性	重要	9.8	なし	なし	RCE
CVE-2022-22013	Windows LDAP 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-2022-22014	Windows LDAP 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-2022-29128	Windows LDAP 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-2022-29129	Windows LDAP 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-2022-29130	Windows LDAP におけるリモートコード実行の脆弱性	重要	9.8	なし	なし	RCE
CVE-2022-29131	Windows LDAP 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-2022-29137	Windows LDAP 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-2022-29139	Windows LDAP 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-2022-29141	Windows LDAP 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-2022-26933	Windows NTFS における情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-22016	Windows PlayToManager における特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-29104	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-2022-29132	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-2022-29114	Windows 印刷スプーラにおける情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-29140	Windows 印刷スプーラにおける情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-29125	Windows プッシュ通知アプリにおける特権昇格の脆弱性	重要	7	なし	なし	EoP
CVE-2022-29103	Windows Remote Access Connection Manager における特権昇格の脆弱性	重要	7.8	なし	なし	EoP
CVE-2022-26930	Windows Remote Access Connection Manager における情報漏えいの脆弱性	重要	5.5	なし	なし	Info
CVE-2022-22015	Windows リモート デスクトップ プロトコル（RDP）における情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-26936	Windows Server Service における情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-29121	Windows WLAN AutoConfig Service におけるサービス拒否の脆弱性	重要	6.5	なし	なし	DoS
CVE-2022-26935	Windows WLAN AutoConfig Service における情報漏えいの脆弱性	重要	6.5	なし	なし	Info
CVE-2022-30130	.NET Framework におけるサービス拒否の脆弱性	低	3.3	なし	なし	DoS

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