

2026年5月にMicrosoftが公開したCVEの一覧

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-35435	Azure AI Foundryの権限昇格の脆弱性	Critical	8.6	なし	なし	EoP
CVE-2026-35428	Azure Cloud Shellのなりすましの脆弱性	Critical	9.6	なし	なし	Spoofing
CVE-2026-42826	Azure DevOpsの情報漏洩の脆弱性	Critical	10	なし	なし	Info
CVE-2026-32207	Azure Machine Learning Notebookのなりすましの脆弱性	Critical	8.8	なし	なし	Spoofing
CVE-2026-33109	Azure Managed Instance for Apache Cassandraのリモートコード実行の脆弱性	Critical	9.9	なし	なし	RCE
CVE-2026-33844	Azure Managed Instance for Apache Cassandraのリモートコード実行の脆弱性	Critical	9	なし	なし	RCE
CVE-2026-41105	Azure Monitor Action Group Notification Systemの権限昇格の脆弱性	Critical	8.1	なし	なし	EoP
CVE-2026-33111	Copilot Chat (Microsoft Edge) の情報漏洩の脆弱性	Critical	7.5	なし	なし	Info
CVE-2026-26129	M365 Copilotの情報漏洩の脆弱性	Critical	7.5	なし	なし	Info
CVE-2026-26164	M365 Copilotの情報漏洩の脆弱性	Critical	7.5	なし	なし	Info
CVE-2026-33821	Microsoft Dynamics 365 Customer Insightsの権限昇格の脆弱性	Critical	7.7	なし	なし	EoP

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-42898	Microsoft Dynamics 365（オンプレミス）のリモートコード実行の脆弱性	Critical	9.9	なし	なし	RCE
CVE-2026-40379	Microsoft Enterprise Security Token Service（ESTS）のなりすましの脆弱性	Critical	9.3	なし	なし	Spoofing
CVE-2026-40363	Microsoft Officeのリモートコード実行の脆弱性	Critical	8.4	なし	なし	RCE
CVE-2026-40358	Microsoft Officeのリモートコード実行の脆弱性	Critical	8.4	なし	なし	RCE
CVE-2026-34327	Microsoft Partner Centerのなりすましの脆弱性	Critical	8.2	なし	なし	Spoofing
CVE-2026-40365	Microsoft SharePoint Serverのリモートコード実行の脆弱性	Critical	8.8	なし	なし	RCE
CVE-2026-41103	Jira & Confluence向けMicrosoft SSOプラグインの権限昇格の脆弱性	Critical	9.1	なし	なし	EoP
CVE-2026-33823	Microsoft Team Events Portalの情報漏洩の脆弱性	Critical	9.6	なし	なし	Info
CVE-2026-40364	Microsoft Wordのリモートコード実行の脆弱性	Critical	8.4	なし	なし	RCE
CVE-2026-40366	Microsoft Wordのリモートコード実行の脆弱性	Critical	8.4	なし	なし	RCE
CVE-2026-40361	Microsoft Wordのリモートコード実行の脆弱性	Critical	8.4	なし	なし	RCE
CVE-2026-40367	Microsoft Wordのリモートコード実行の脆弱性	Critical	8.4	なし	なし	RCE

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-42831	Office for Androidのリモートコード実行の脆弱性	Critical	7.8	なし	なし	RCE
CVE-2026-41096	Windows DNSクライアントのリモートコード実行の脆弱性	Critical	9.8	なし	なし	RCE
CVE-2026-35421	Windows GDIのリモートコード実行の脆弱性	Critical	7.8	なし	なし	RCE
CVE-2026-40403	Windows Graphicsコンポーネントのリモートコード実行の脆弱性	Critical	8.8	なし	なし	RCE
CVE-2026-40402	Windows Hyper-Vの権限昇格の脆弱性	Critical	9.3	なし	なし	EoP
CVE-2026-32161	Windows Native WiFi Miniportドライバのリモートコード実行の脆弱性	Critical	7.5	なし	なし	RCE
CVE-2026-41089	Windows Netlogonのリモートコード実行の脆弱性	Critical	9.8	なし	なし	RCE
CVE-2026-32175	.NET Coreの改ざんの脆弱性	Important	4.3	なし	なし	Tampering
CVE-2026-32177	.NETの権限昇格の脆弱性	Important	7.3	なし	なし	EoP
CVE-2026-35433	.NETの権限昇格の脆弱性	Important	7.3	なし	なし	EoP
CVE-2025-54518 *	AMD: CVE-2025-54518 CPU OP Cacheの破損	Important		なし	なし	RCE
CVE-2026-42899	ASP.NET Coreのサービス拒否の脆弱性	Important	7.5	なし	なし	DoS

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-40381	Azure Connected Machineエージェントの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-42823 †	Azure Logic Appsの権限昇格の脆弱性	Important	9.9	なし	なし	EoP
CVE-2026-33833	Azure Machine Learning Notebookのなりすましの脆弱性	Important	8.2	なし	なし	Spoofing
CVE-2026-32204	Azure Monitor Agentの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-42830	Azure Monitor Agent Metrics Extensionの権限昇格の脆弱性	Important	6.5	なし	なし	EoP
CVE-2026-33117	Azure SDK for Javaのセキュリティ機能のバイパスの脆弱性	Important	9.1	なし	なし	SFB
CVE-2026-41109	GitHub CopilotおよびVisual Studio Codeのセキュリティ機能のバイパスの脆弱性	Important	8.8	なし	なし	SFB
CVE-2026-35424	Internet Key Exchange (IKE) プロトコルのサービス拒否の脆弱性	Important	7.5	なし	なし	DoS
CVE-2026-41614	M365 Copilot for Desktopのなりすましの脆弱性	Important	6.2	なし	なし	Spoofing
CVE-2026-41100	Microsoft 365 Copilot for Androidのなりすましの脆弱性	Important	4.4	なし	なし	Spoofing
CVE-2026-40377	Microsoft Cryptographic Servicesの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-41094	Microsoft Data Formulatorのリモートコード実行の脆弱性	Important	8.8	なし	なし	RCE

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-40417	Microsoft Dynamics 365 Business Centralの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-42833	Microsoft Dynamics 365(オンプレミス)のリモートコード実行の脆弱性	Important	9.1	なし	なし	RCE
CVE-2026-42838	Microsoft Edge (Chromiumベース)の権限昇格の脆弱性	Important	5.4	なし	なし	EoP
CVE-2026-40360	Microsoft Excelの情報漏洩の脆弱性	Important	7.8	なし	なし	Info
CVE-2026-40359	Microsoft Excelのリモートコード実行の脆弱性	Important	7.8	なし	なし	RCE
CVE-2026-40362	Microsoft Excelのリモートコード実行の脆弱性	Important	7.8	なし	なし	RCE
CVE-2026-42832	Microsoft Excelのなりすましの脆弱性	Important	7.7	なし	なし	Spoofing
CVE-2026-34329	Microsoft Message Queuing (MSMQ) のリモートコード実行の脆弱性	Important	8.8	なし	なし	RCE
CVE-2026-40419	Microsoft Office Click-To-Runの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-40418	Microsoft Office Click-To-Runの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-35436	Microsoft Office Click-To-Runの権限昇格の脆弱性	Important	8.8	なし	なし	EoP
CVE-2026-40420	Microsoft Office Click-To-Runの権限昇格の脆弱性	Important	8.8	なし	なし	EoP

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-42893	Microsoft Outlook for iOSの改ざんの脆弱性	Important	7.4	なし	なし	Tampering
CVE-2026-40374	Microsoft Power Automate Desktopの情報漏洩の脆弱性	Important	6.5	なし	なし	Info
CVE-2026-41102	Microsoft PowerPoint for Androidのなりすましの脆弱性	Important	7.1	なし	なし	Spoofing
CVE-2026-35439	Microsoft SharePoint Serverのリモートコード実行の脆弱性	Important	8.8	なし	なし	RCE
CVE-2026-40368	Microsoft SharePoint Serverのリモートコード実行の脆弱性	Important	8	なし	なし	RCE
CVE-2026-33110	Microsoft SharePoint Serverのリモートコード実行の脆弱性	Important	8.8	なし	なし	RCE
CVE-2026-33112	Microsoft SharePoint Serverのリモートコード実行の脆弱性	Important	8.8	なし	なし	RCE
CVE-2026-40357	Microsoft SharePoint Serverのリモートコード実行の脆弱性	Important	8.8	なし	なし	RCE
CVE-2026-32185	Microsoft Teamsのなりすましの脆弱性	Important	5.5	なし	なし	Spoofing
CVE-2026-41101	Microsoft Word for Androidのなりすましの脆弱性	Important	7.1	なし	なし	Spoofing
CVE-2026-35440	Microsoft Wordの情報漏洩の脆弱性	Important	5.5	なし	なし	Info
CVE-2026-40421	Microsoft Wordの情報漏洩の脆弱性	Important	4.3	なし	なし	Info

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-41097	Secure Bootのセキュリティ機能のバイパスの脆弱性	Important	6.7	なし	なし	SFB
CVE-2026-40370 †	SQL Serverのリモートコード実行の脆弱性	Important	8.8	なし	なし	RCE
CVE-2026-41613	Visual Studio Codeの権限昇格の脆弱性	Important	8.8	なし	なし	EoP
CVE-2026-41612	Visual Studio Codeの情報漏洩の脆弱性	Important	5.5	なし	なし	Info
CVE-2026-41611	Visual Studio Codeのリモートコード実行の脆弱性	Important	7.8	なし	なし	RCE
CVE-2026-41610	Visual Studio Codeのセキュリティ機能のバイパスの脆弱性	Important	6.3	なし	なし	SFB
CVE-2026-33839	Win32kの権限昇格の脆弱性	Important	7	なし	なし	EoP
CVE-2026-33840	Win32kの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34330	Win32kの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34331	Win32kの権限昇格の脆弱性	Important	7	なし	なし	EoP
CVE-2026-35423	Windows 11 Telnetクライアントの情報漏洩の脆弱性	Important	5.4	なし	なし	Info
CVE-2026-35438	Windows Admin Centerの権限昇格の脆弱性	Important	8.3	なし	なし	EoP

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-41086	Azure Portal上のWindows Admin Centerの権限昇格の脆弱性	Important	8.8	なし	なし	EoP
CVE-2026-34344	WinSock向けWindows Ancillary Function Driverの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34345	WinSock向けWindows Ancillary Function Driverの権限昇格の脆弱性	Important	7	なし	なし	EoP
CVE-2026-35416	WinSock向けWindows Ancillary Function Driverの権限昇格の脆弱性	Important	7	なし	なし	EoP
CVE-2026-41088	WinSock向けWindows Ancillary Function Driverの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34343	Windows Application Identity (AppID) サブシステムの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-35418	Windows Cloud Files Mini Filterドライバの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-33835	Windows Cloud Files Mini Filterドライバの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34337	Windows Cloud Files Mini Filterドライバの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-40407	Windows Common Log File Systemドライバの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-40397	Windows Common Log File Systemドライバの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-42896	Windows DWM Coreライブラリの権限昇格の脆弱性	Important	7.8	なし	なし	EoP

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-35419	Windows DWM Coreライブラリの情報漏洩の脆弱性	Important	5.5	なし	なし	Info
CVE-2026-34336	Windows DWM Coreライブラリの情報漏洩の脆弱性	Important	7.8	なし	なし	Info
CVE-2026-33834	Windows イベントログサービスの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-32209	Windows Filtering Platform (WFP) のセキュリティ機能のバイパスの脆弱性	Important	4.4	なし	なし	SFB
CVE-2026-33841	Windows カーネルの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-35420	Windows カーネルの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-40369	Windows カーネルの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34332	Windows カーネルモードドライバのリモートコード実行の脆弱性	Important	8	なし	なし	RCE
CVE-2026-34339	Windows Lightweight Directory Access Protocol (LDAP) のサービス拒否の脆弱性	Important	5.5	なし	なし	DoS
CVE-2026-34341	Windows Link-Layer Discovery Protocol (LLDP) の権限昇格の脆弱性	Important	7	なし	なし	EoP
CVE-2026-33838	Windows Message Queuing (MSMQ) の権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34342	Windows Print Spoolerの権限昇格の脆弱性	Important	7	なし	なし	EoP

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-41095	Windows Projected File Systemの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34340	Windows Projected File Systemの権限昇格の脆弱性	Important	7	なし	なし	EoP
CVE-2026-40398	Windowsリモートデスクトップサービスの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-21530	Windows Rich Text Editの権限昇格の脆弱性	Important	6.7	なし	なし	EoP
CVE-2026-32170	Windows Rich Text Editの権限昇格の脆弱性	Important	6.7	なし	なし	EoP
CVE-2026-40410	Windows SMBクライアントの権限昇格の脆弱性	Important	7	なし	なし	EoP
CVE-2026-35415	Windows Storage Spaces Controllerの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34350	Windows Storport Miniportドライバのサービス拒否の脆弱性	Important	6.5	なし	なし	DoS
CVE-2026-40405	Windows TCP/IPのサービス拒否の脆弱性	Important	7.5	なし	なし	DoS
CVE-2026-40414	Windows TCP/IPのサービス拒否の脆弱性	Important	7.4	なし	なし	DoS
CVE-2026-40401	Windows TCP/IPのサービス拒否の脆弱性	Important	6.2	なし	なし	DoS
CVE-2026-40413	Windows TCP/IPのサービス拒否の脆弱性	Important	7.4	なし	なし	DoS

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-35422	Windows TCP/IPドライバのセキュリティ機能のバイパスの脆弱性	Important	6.5	なし	なし	SFB
CVE-2026-34351	Windows TCP/IPの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-40399	Windows TCP/IPの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34334	Windows TCP/IPの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-40406	Windows TCP/IPの情報漏洩の脆弱性	Important	7.5	なし	なし	Info
CVE-2026-33837	Windows TCP/IPのローカル権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-40415	Windows TCP/IPのリモートコード実行の脆弱性	Important	8.1	なし	なし	RCE
CVE-2026-42825	Windowsテレフォニーサービスの権限昇格の脆弱性	Important	7	なし	なし	EoP
CVE-2026-34338	Windowsテレフォニーサービスの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-40382	Windowsテレフォニーサービスの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-40380	Windows Volume Manager Extensionドライバのリモートコード実行の脆弱性	Important	6.2	なし	なし	RCE
CVE-2026-40408	Windows WAN ARPドライバの権限昇格の脆弱性	Important	7.8	なし	なし	EoP

CVE	タイトル	深刻度	CVSS	公開済み	悪用	種類
CVE-2026-34333	Windows Win32kの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-34347	Windows Win32kの権限昇格の脆弱性	Important	7	なし	なし	EoP
CVE-2026-35417	Windows Win32kの権限昇格の脆弱性	Important	7.8	なし	なし	EoP
CVE-2026-42891	Microsoft Edge (Chromiumベース) for Androidのなりすましの脆弱性	Moderate	6.5	なし	なし	Spoofing
CVE-2026-35429	Microsoft Edge (Chromiumベース) for Androidのなりすましの脆弱性	Moderate	4.3	なし	なし	Spoofing
CVE-2026-41107	Microsoft Edge (Chromiumベース) の情報漏洩の脆弱性	Moderate	7.4	なし	なし	Info
CVE-2026-40416	Microsoft Edge (Chromiumベース) for Androidのなりすましの脆弱性	Low	4.3	なし	なし	Spoofing

* このCVEは第三者によって既に公開されており、今回Microsoftのリリースにも含まれるようになったことを示します。

† 脆弱性に完全に対処するためには、追加の管理者作業が必要であることを示します。