Microsoft 2026年7月セキュリティアップデート一覧

621件のCVE | CVE番号をクリックするとMicrosoft Security Response Centerの各脆弱性ページを開きます。

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-56155	Active Directory Federation Servicesの特権昇格の脆弱性	重要	7.8	いいえ	はい	特権昇格 (EoP)
CVE-2026-56164	Microsoft SharePoint Serverの特権昇格の脆弱性	警告	5.3	いいえ	はい	特権昇格 (EoP)
CVE-2026-50661	Windows BitLockerのセキュリティ機能のバイパスの脆弱性	重要	6.1	はい	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-54121	Active Directory Certificate Servicesの特権昇格の脆弱性	緊急	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-45499 ※	Azure OpenAIの特権昇格の脆弱性	緊急	9.9	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-48564	DHCP Server Serviceのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50370	DHCP Server Serviceのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-56159	DHCP Server Serviceのリモートコード実行の脆弱性	緊急	9.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50382	DirectX Graphics Kernelのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-41106 ※	Microsoft 365 Copilotの特権昇格の脆弱性	緊急	9.3	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-26145 ※	Microsoft Azure Synapseの特権昇格の脆弱性	緊急	4.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-48561	Microsoft Copilotのリモートコード実行の脆弱性	緊急	9.6	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55011	Microsoft Defenderのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55012	Microsoft Defenderのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55944	Microsoft Dynamics NAV and Microsoft Dynamics 365 Business Central (On Premises)のリモートコード実行の脆弱性	緊急	9.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57100 ※	Microsoft Entra Provisioning Serviceの特権昇格の脆弱性	緊急	9.9	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-55041	Microsoft Excelのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-54998 ※	Microsoft Exchange Onlineの特権昇格の脆弱性	緊急	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-55008	Microsoft Exchange Serverのなりすましの脆弱性	緊急	9.6	いいえ	いいえ	なりすまし

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-54992	Microsoft Message Queuing Queue Managerのリモートコード実行の脆弱性	緊急	8.4	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50314	Microsoft Officeのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50467	Microsoft Officeのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55018	Microsoft Officeのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55022	Microsoft Officeのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55045	Microsoft Officeのリモートコード実行の脆弱性	緊急	8.4	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55049	Microsoft Officeのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55129	Microsoft Officeのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55056	Microsoft Officeのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55140	Microsoft Officeのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55043	Microsoft PowerPointのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55123	Microsoft PowerPointのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55120	Microsoft PowerPointのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50522	Microsoft SharePointのリモートコード実行の脆弱性	緊急	9.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58644	Microsoft SharePointのリモートコード実行の脆弱性	緊急	9.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55040	Microsoft SharePoint Serverのセキュリティ機能のバイパスの脆弱性	緊急	9.1	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-54117	Microsoft SQL Serverのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-54118	Microsoft SQL Serverのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50655	Microsoft Windows Media Foundationのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-56189	Microsoft Windows Media Foundationのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57090	Microsoft Windows Media Foundationのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-57094	Microsoft Windows Media Foundationのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57087	Microsoft Windows Media Foundationのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57092	Microsoft Windows VMSwitchの特権昇格の脆弱性	緊急	9.9	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-55033	Microsoft Wordのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55127	Microsoft Wordのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55132	Microsoft Wordのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55010	Minecraft Bedrock Dedicated Serverのリモートコード実行の脆弱性	緊急	9.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50474	Remote Desktop Clientのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49164	Windows Active Directory Domain Servicesのリモートコード実行の脆弱性	緊急	8.1	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-54128	Windows DHCP Clientのリモートコード実行の脆弱性	緊急	8.4	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50518	Windows DHCP Serverのリモートコード実行の脆弱性	緊急	9.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49796	Windows GDI+のリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50380	Windows GDI+のリモートコード実行の脆弱性	緊急	9.6	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-54127	Windows Hyper-Vの特権昇格の脆弱性	緊急	7.4	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50680	Windows Hyper-Vの特権昇格の脆弱性	緊急	8.2	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50327	Windows Mediaのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58542	Windows Mediaのリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58608	Windows Print Spoolerのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-54982	Windows Reliable Multicast Transport Driver (RMCAST)のリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-54995	Windows Reliable Multicast Transport Driver (RMCAST)のリモートコード実行の脆弱性	緊急	8.1	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-42982	Windows Secure Kernel Modeの特権昇格の脆弱性	緊急	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50392	Windows Secure Kernel Modeの特権昇格の脆弱性	緊急	7	いいえ	いいえ	特権昇格 (EoP)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-50694	Windows Secure Socket Tunneling Protocol (SSTP)のリモートコード実行の脆弱性	緊急	8.1	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-56188	Windows Server Network driverのリモートコード実行の脆弱性	緊急	9.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50444	Windows Server Update Service (WSUS)の特権昇格の脆弱性	緊急	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54999	Windows TCP/IPのリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-47302	.NETのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50525	.NETのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50651	.NETのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-57108	.NETのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50524	.NET Frameworkのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50527	.NET Frameworkのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50648	.NET Frameworkのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50650	.NET Frameworkの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50646	.NET Frameworkのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50649	.NETのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-47304	.NETのセキュリティ機能のバイパスの脆弱性	重要	8.1	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-50528	.NETのセキュリティ機能のバイパスの脆弱性	重要	8.2	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-50659	.NETのなりすましの脆弱性	重要	6.5	いいえ	いいえ	なりすまし
CVE-2026-50526	.NETの改ざんの脆弱性	重要	7	いいえ	いいえ	改ざん
CVE-2026-50682	Active Directoryのサービス拒否 (DoS) の脆弱性	重要	7.1	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-55001	Active Directory Domain Servicesの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50647	Active Directory Federation Serverのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50684	Active Directory Federation Serverのなりすましの脆弱性	重要	4.8	いいえ	いいえ	なりすまし

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-56170	ASP.NET Coreのサービス拒否（DoS）の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-47300	ASP.NET Coreの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-47303	ASP.NET Coreの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50652	Azure Active Directoryのサービス拒否（DoS）の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-50653	Azure Active Directoryのサービス拒否（DoS）の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-57969	Azure CycleCloudの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-58279	Azure CycleCloudの特権昇格の脆弱性	重要	6.5	いいえ	いいえ	特権昇格（EoP）
CVE-2026-47632	Azure Monitor Agent Metrics Extensionの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50338	Azure Spring Appsの特権昇格の脆弱性	重要	8.2	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50488	Clipboard User Serviceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50491	Code Integrity DLL (ci.dll)の特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50381	Composite Image File System driver (cimfs.sys)の情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50427	Content Delivery Managerの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50692	Desktop Window Managerの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-58633	Desktop Window Managerの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-58634	Desktop Window Managerの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50296	DirectX Graphics Kernelの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50375	DirectX Graphics Kernelの特権昇格の脆弱性	重要	6.3	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50353	DirectX Graphics Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50493	DirectX Graphics Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-56643	DirectX Graphics Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-56644	DirectX Graphics Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格（EoP）

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-58629	DirectX Graphics Kernelの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49174	DNS Clientの改ざんの脆弱性	重要	6.1	いいえ	いいえ	改ざん
CVE-2026-50495	DNS Clientの改ざんの脆弱性	重要	6.1	いいえ	いいえ	改ざん
CVE-2026-57088	Extensible Storage Engine (ESENT)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50663	Game: Age of Empires II: Definitive Editionのリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-47282	GitHub Copilot and Visual Studio Codeの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-41109	GitHub Copilot and Visual Studio Codeのセキュリティ機能のバイパスの脆弱性	重要	8.8	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-50510	GitHub Copilotのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49787	HTTP.sysのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50420	HTTP.sysの情報漏洩の脆弱性	重要	6.2	いいえ	いいえ	情報漏洩
CVE-2026-49788	HTTP/2のサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50696	Internet Key Exchange (IKE) Protocolのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-58617	M365 Copilot for iOSの特権昇格の脆弱性	重要	8.1	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58595	Microsoft Bing App for IOSのなりすましの脆弱性	重要	8.1	いいえ	いいえ	なりすまし
CVE-2026-49162	Microsoft Brokering File Systemの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50305	Microsoft Brokering File Systemの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50361	Microsoft Brokering File Systemの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50466	Microsoft Brokering File Systemの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50458	Microsoft Brokering File Systemの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50658	Microsoft Defender for Endpoint for Macの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56178	Microsoft Defender for Endpoint for Macの特権昇格の脆弱性	重要	5.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50657	Microsoft Defender for Endpoint for Macの情報漏洩の脆弱性	重要	4.7	いいえ	いいえ	情報漏洩
CVE-2026-50329	Microsoft DWM Core Libraryの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-58541	Microsoft DWM Core Libraryの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58596	Microsoft Edge (Chromium-based)の特権昇格の脆弱性	重要	8.3	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-57991	Microsoft Edge (Chromium-based)の情報漏洩の脆弱性	重要	7.4	いいえ	いいえ	情報漏洩
CVE-2026-58291	Microsoft Edge (Chromium-based)の情報漏洩の脆弱性	重要	6.1	いいえ	いいえ	情報漏洩
CVE-2026-57981	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57984	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57985	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	7.6	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57986	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57988	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	7.1	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57992	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58276	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-56645	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57974	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57975	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58281	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	8.3	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58284	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	8.3	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58285	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	8.3	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58287	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	8.3	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58288	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	8.3	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58289	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	9	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58290	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58292	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-58293	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	8.1	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58294	Microsoft Edge (Chromium-based)のリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57983	Microsoft Edge (Chromium-based)のセキュリティ機能のバイパスの脆弱性	重要	8.7	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-58295	Microsoft Edge (Chromium-based)のセキュリティ機能のバイパスの脆弱性	重要	8.3	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-58525	Microsoft Edge (Chromium-based)のセキュリティ機能のバイパスの脆弱性	重要	8.2	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-57987	Microsoft Edge (Chromium-based)のなりすましの脆弱性	重要	6.5	いいえ	いいえ	なりすまし
CVE-2026-58278	Microsoft Edge (Chromium-based)のなりすましの脆弱性	重要	5.4	いいえ	いいえ	なりすまし
CVE-2026-56646	Microsoft Edge (Chromium-based)のなりすましの脆弱性	重要	6.5	いいえ	いいえ	なりすまし
CVE-2026-57977	Microsoft Edge (Chromium-based)のなりすましの脆弱性	重要	7.1	いいえ	いいえ	なりすまし
CVE-2026-57993	Microsoft Edge (Chromium-based)のなりすましの脆弱性	重要	7.4	いいえ	いいえ	なりすまし
CVE-2026-58282	Microsoft Edge (Chromium-based)のなりすましの脆弱性	重要	8.1	いいえ	いいえ	なりすまし
CVE-2026-58283	Microsoft Edge (Chromium-based)のなりすましの脆弱性	重要	8.1	いいえ	いいえ	なりすまし
CVE-2026-58286	Microsoft Edge (Chromium-based)のなりすましの脆弱性	重要	8.1	いいえ	いいえ	なりすまし
CVE-2026-58298	Microsoft Edge (Chromium-based)のなりすましの脆弱性	重要	7.2	いいえ	いいえ	なりすまし
CVE-2026-58524	Microsoft Edge (Chromium-based)のなりすましの脆弱性	重要	5.4	いいえ	いいえ	なりすまし
CVE-2026-58296	Microsoft Edge for Androidの情報漏洩の脆弱性	重要	7.1	いいえ	いいえ	情報漏洩
CVE-2026-58297	Microsoft Edge for Androidの情報漏洩の脆弱性	重要	7.1	いいえ	いいえ	情報漏洩
CVE-2026-58300	Microsoft Edge for Androidの情報漏洩の脆弱性	重要	6.2	いいえ	いいえ	情報漏洩
CVE-2026-58522	Microsoft Edge for Androidの情報漏洩の脆弱性	重要	6.8	いいえ	いいえ	情報漏洩
CVE-2026-58299	Microsoft Edge for Androidのリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58523	Microsoft Edge for Androidのセキュリティ機能のバイパスの脆弱性	重要	6.5	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-50678	Microsoft Excelの情報漏洩の脆弱性	重要	6.6	いいえ	いいえ	情報漏洩
CVE-2026-54988	Microsoft Excelの情報漏洩の脆弱性	重要	6.1	いいえ	いいえ	情報漏洩
CVE-2026-48580	Microsoft Excelの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50408	Microsoft Excelの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55046	Microsoft Excelの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55138	Microsoft Excelの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55054	Microsoft Excelの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-55122	Microsoft Excelの情報漏洩の脆弱性	重要	7.1	いいえ	いいえ	情報漏洩
CVE-2026-55898	Microsoft Excelの情報漏洩の脆弱性	重要	6.1	いいえ	いいえ	情報漏洩
CVE-2026-50675	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55899	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55948	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-58618	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-47642	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55024	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55025	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55031	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55048	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55029	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55039	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55136	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55141	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55036	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55044	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55037	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55058	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55137	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55053	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)
CVE-2026-55131	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行(RCE)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-54131	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55947	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55949	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-56156	Microsoft Excelのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55006	Microsoft Exchange Serverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-55009	Microsoft Exchange Serverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-55005	Microsoft Exchange Serverのリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-56642	Microsoft Fabric Data Warehouseのリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50343	Microsoft Install Serviceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50439	Microsoft Message Queuing Queue Managerのリモートコード実行の脆弱性	重要	8.1	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58537	Microsoft NAT Helper Components (ipnathlp.dll)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56193	Microsoft Officeの情報漏洩の脆弱性	重要	7.1	いいえ	いいえ	情報漏洩
CVE-2026-55023	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55026	Microsoft Officeの情報漏洩の脆弱性	重要	6.2	いいえ	いいえ	情報漏洩
CVE-2026-55027	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55028	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55047	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55035	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55057	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55121	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55042	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55139	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50665	Microsoft Officeの情報漏洩の脆弱性	重要	7.8	いいえ	いいえ	情報漏洩
CVE-2026-56192	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-56195	Microsoft Officeの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-47290	Microsoft Officeのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50301	Microsoft Officeのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-55017	Microsoft Officeのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55125	Microsoft Officeのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55133	Microsoft OneNoteのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58636	Microsoft PC Managerの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50438	Microsoft PC Managerの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58647	Microsoft PowerBI Report Serverのなりすましの脆弱性	重要	8	いいえ	いいえ	なりすまし
CVE-2026-55052	Microsoft SharePointの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58277	Microsoft SharePointの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-55051	Microsoft SharePoint Serverの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-54108	Microsoft SharePoint Serverのなりすましの脆弱性	重要	6.5	いいえ	いいえ	なりすまし
CVE-2026-55016	Microsoft SharePoint Serverのなりすましの脆弱性	重要	4.6	いいえ	いいえ	なりすまし
CVE-2026-55019	Microsoft SharePoint Serverのなりすましの脆弱性	重要	4.6	いいえ	いいえ	なりすまし
CVE-2026-55020	Microsoft SharePoint Serverのなりすましの脆弱性	重要	4.6	いいえ	いいえ	なりすまし
CVE-2026-55021	Microsoft SharePoint Serverのなりすましの脆弱性	重要	7.3	いいえ	いいえ	なりすまし
CVE-2026-55030	Microsoft SharePoint Serverのなりすましの脆弱性	重要	4.6	いいえ	いいえ	なりすまし
CVE-2026-55034	Microsoft SharePoint Serverのなりすましの脆弱性	重要	7.3	いいえ	いいえ	なりすまし
CVE-2026-55126	Microsoft SharePoint Serverのなりすましの脆弱性	重要	7.3	いいえ	いいえ	なりすまし
CVE-2026-55135	Microsoft SharePoint Serverのなりすましの脆弱性	重要	4.6	いいえ	いいえ	なりすまし
CVE-2026-56157	Microsoft SharePoint Serverのなりすましの脆弱性	重要	5.4	いいえ	いいえ	なりすまし
CVE-2026-47296	Microsoft SQL Serverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-55002	Microsoft SQL Serverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-47295	Microsoft SQL Serverの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50468	Microsoft SQL Serverの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-54116	Microsoft SQL Serverの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-42900	Microsoft Windows App Storeの特権昇格の脆弱性	重要	8.1	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49784	Microsoft Windows App Storeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50356	Microsoft Windows App Storeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-49165	Microsoft Windows App Storeの情報漏洩の脆弱性	重要	7.1	いいえ	いいえ	情報漏洩
CVE-2026-54993	Microsoft Windows Media Foundationのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58610	Microsoft Windows Media Foundationのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55050	Microsoft Wordの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55124	Microsoft Wordの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55142	Microsoft Wordの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-55032	Microsoft Wordのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55055	Microsoft Wordのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55038	Microsoft Wordのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55134	Microsoft Wordのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55128	Microsoft Wordのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55130	Microsoft Wordのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50359	Microsoft XML Core Servicesの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-57097	Microsoft XMLのセキュリティ機能のバイパスの脆弱性	重要	6.4	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-50346	Netlogon RPCの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50402	NTFSの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50506	OData for ASP.NET and ASP.NET Coreのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-45646	OData for ASP.NET and ASP.NET Coreのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-54989	Quality Windows Audio/Video Experience (QWAVE)の特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50365	Remote Access Management service/API (RPC server)の特権昇格の脆弱性	重要	8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54990	Remote Desktop Clientのリモートコード実行の脆弱性	重要	9.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58594	Remote Desktop Clientのリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-56190	Remote Desktop Protocolのリモートコード実行の脆弱性	重要	9.8	いいえ	いいえ	リモートコード実行 (RCE)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-49783	Secure Bootのセキュリティ機能のバイパスの脆弱性	重要	7.8	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-42990	SQL Server ODBC driverの特権昇格の脆弱性	重要	9.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49168	Storage Spaces Directの特権昇格の脆弱性	重要	6.2	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-48581	Surface Broker SDMAの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49180	Universal Plug and Play (upnp.dll)の情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50455	Universal Plug and Play (upnp.dll)の情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-54111	Universal Print Management Serviceの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58543	Universal Print Management Serviceの特権昇格の脆弱性	重要	6.3	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58601	Virtual Hard Disk (VHD) Miniport Driverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50520	Visual Studio Codeのリモートコード実行の脆弱性	重要	8.4	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-45496	Visual Studio Codeのセキュリティ機能のバイパスの脆弱性	重要	5.5	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-57101	Visual Studio Codeのセキュリティ機能のバイパスの脆弱性	重要	7.1	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-57102	Visual Studio Codeのセキュリティ機能のバイパスの脆弱性	重要	8.8	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-47305	Visual Studioのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49805	Win32kの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50297	Win32kの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50325	Win32kの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50489	Win32kの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-57095	Win32kの特権昇格の脆弱性	重要	6.2	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50416	Win32kの情報漏洩の脆弱性	重要	3.3	いいえ	いいえ	情報漏洩
CVE-2026-56184	Win32kの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50432	Window Virtual Filtering Platform (VFP)のサービス拒否 (DoS) の脆弱性	重要	5.3	いいえ	いいえ	サービス拒否 (DoS)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-54119	Windows Active Directoryのサービス拒否（DoS）の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-57976	Windows Active Directory Domain Servicesのサービス拒否（DoS）の脆弱性	重要	6.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-50366	Windows Active Directory Domain Servicesのサービス拒否（DoS）の脆弱性	重要	6.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-49178	Windows Active Directory Domain Servicesのリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行（RCE）
CVE-2026-58529	Windows Active Directory Federation Services (ADFS)の情報漏洩の脆弱性	重要	7.1	いいえ	いいえ	情報漏洩
CVE-2026-54983	Windows Active Directory Federation Servicesのサービス拒否（DoS）の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-50695	Windows Active Directory Federation Servicesのサービス拒否（DoS）の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-50304	Windows Active Directory Federation Servicesのサービス拒否（DoS）の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-50368	Windows Active Directory Federation Servicesのサービス拒否（DoS）の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-50324	Windows Active Directory Federation Servicesのサービス拒否（DoS）の脆弱性	重要	5.9	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-50355	Windows Active Directory Federation Servicesのサービス拒否（DoS）の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-50411	Windows Active Directory Federation Servicesのサービス拒否（DoS）の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-58631	Windows Admin Center (WAC)のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行（RCE）
CVE-2026-56196	Windows Admin Center (WAC)のリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行（RCE）
CVE-2026-56197	Windows Admin Center (WAC)のリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行（RCE）
CVE-2026-56169	Windows Admin Centerの特権昇格の脆弱性	重要	8.1	いいえ	いいえ	特権昇格（EoP）
CVE-2026-57107	Windows Admin Centerの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-56185	Windows Admin Centerの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-50312	Windows Ancillary Function Driver for WinSockの特権昇格の脆弱性	重要	4.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50462	Windows Ancillary Function Driver for WinSockの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-57093	Windows Ancillary Function Driver for WinSockの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-34346	Windows Ancillary Function Driver for WinSockの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-48572	Windows App Package Installerの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-48571	Windows App Package Installerの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50400	Windows App Package Installerの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50331	Windows Application Model Core APIの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49803	Windows AppX Deployment Extensionsの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50351	Windows Audio Compression Manager (ACM)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50440	Windows Audio Serviceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-34328	Windows Audio Serviceの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50406	Windows Backup Engineの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50364	Windows Backup Serviceの特権昇格の脆弱性	重要	7.3	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-42975	Windows Bluetooth Port Driverのリモートコード実行の脆弱性	重要	8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58538	Windows Bluetooth Serviceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58638	Windows Boot Loaderのセキュリティ機能のバイパスの脆弱性	重要	6	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-58637	Windows Client-Side Cachingの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50384	Windows Clip Serviceの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49183	Windows Clipboard Serverの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50689	Windows Clipboard Serverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50374	Windows Cloud Files Mini Filter Driverの特権昇格の脆弱性	重要	6.3	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58536	Windows Cloud Files Mini Filter Driverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58613	Windows Cloud Files Mini Filter Driverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50401	Windows Cloud Files Mini Filter Driverの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50697	Windows Common Log File System Driverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50667	Windows Common Log File System Driverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-50421	Windows Connected User Experiences and Telemetryの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50428	Windows Container Isolation FS Filter Driver (unionfs.sys)の情報漏洩の脆弱性	重要	7.1	いいえ	いいえ	情報漏洩
CVE-2026-50352	Windows Cryptographic Servicesの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50302	Windows Cryptographic Servicesのセキュリティ機能のバイパスの脆弱性	重要	4.2	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-55144	Windows Cryptography API: Next Generation (CNG)の改ざんの脆弱性	重要	7.1	いいえ	いいえ	改ざん
CVE-2026-50347	Windows Data.dllのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49181	Windows DHCP Clientの特権昇格の脆弱性	重要	7.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50683	Windows DHCP Clientの特権昇格の脆弱性	重要	8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58627	Windows DHCP Serverのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50685	Windows DHCP Serverのリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49807	Windows DirectXの情報漏洩の脆弱性	重要	6.2	いいえ	いいえ	情報漏洩
CVE-2026-49175	Windows DNS Clientの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50487	Windows DNS Clientの特権昇格の脆弱性	重要	8.1	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50465	Windows DNS Clientの改ざんの脆弱性	重要	7.1	いいえ	いいえ	改ざん
CVE-2026-49169	Windows DNS Serverのリモートコード実行の脆弱性	重要	8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50426	Windows DNS Serverのリモートコード実行の脆弱性	重要	6.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50424	Windows Domain Controllerのサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50300	Windows DWM Core Libraryの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50437	Windows DWM Core Libraryの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-34348	Windows Event Logging Serviceの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-50502	Windows Event Logging Serviceのリモートコード実行の脆弱性	重要	8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-33842	Windows File Explorerの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-40422	Windows File Explorerの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-41087	Windows File Explorerの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50473	Windows File Explorerの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50442	Windows File Explorerの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-50389	Windows File Explorerの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50456	Windows File Explorerの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-57084	Windows File Explorerの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-57091	Windows File History Serviceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50405	Windows Filtering Platformの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49172	Windows FTP Serviceのリモートコード実行の脆弱性	重要	9.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50387	Windows GDIの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54122	Windows GDI+のリモートコード実行の脆弱性	重要	8.4	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50483	Windows Graphics Componentの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-58609	Windows Graphics Componentのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50391	Windows Group Policyの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50310	Windows Human Interface Deviceの情報漏洩の脆弱性	重要	4.7	いいえ	いいえ	情報漏洩
CVE-2026-50485	Windows Hyper-Vのサービス拒否 (DoS) の脆弱性	重要	4.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-54129	Windows Hyper-Vの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50315	Windows Image Acquisitionの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58534	Windows Input Method Editor (IME)の特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50490	Windows Installerの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58540	Windows Installerの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50425	Windows Internal System User Profileの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50293	Windows Internal Task Barの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49167	Windows Kernelの特権昇格の脆弱性	重要	4.7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49173	Windows Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54132	Windows Kernelの特権昇格の脆弱性	重要	6.8	いいえ	いいえ	特権昇格 (EoP)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-49795	Windows Kernelの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49798	Windows Kernelの特権昇格の脆弱性	重要	9.3	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49808	Windows Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50354	Windows Kernelの特権昇格の脆弱性	重要	7.1	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50332	Windows Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50377	Windows Kernelの特権昇格の脆弱性	重要	5.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50390	Windows Kernelの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50423	Windows Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50397	Windows Kernelの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50436	Windows Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50399	Windows Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50459	Windows Kernelの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50477	Windows Kernelの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50478	Windows Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50484	Windows Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50673	Windows Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58532	Windows Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50294	Windows Kernelの情報漏洩の脆弱性	重要	6.2	いいえ	いいえ	情報漏洩
CVE-2026-50316	Windows Kernelの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50419	Windows Kernelの情報漏洩の脆弱性	重要	3.3	いいえ	いいえ	情報漏洩
CVE-2026-50463	Windows Kernelの情報漏洩の脆弱性	重要	7.5	いいえ	いいえ	情報漏洩
CVE-2026-50475	Windows Kernelの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50429	Windows Kernelの情報漏洩の脆弱性	重要	8.2	いいえ	いいえ	情報漏洩

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-58614	Windows Kernelのセキュリティ機能のバイパスの脆弱性	重要	5.5	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-58545	Windows Kernelのセキュリティ機能のバイパスの脆弱性	重要	5.5	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-58602	Windows Kernel-Mode Driverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50393	Windows Kernel-Mode Driverの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50396	Windows Kernel-Mode Driverの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50378	Windows Key Guardの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50303	Windows Key Guardのセキュリティ機能のバイパスの脆弱性	重要	5.5	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-40378	Windows Local Security Authority Subsystem Service (LSASS)のサービス拒否 (DoS) の脆弱性	重要	7.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-49799	Windows Local Security Authority Subsystem Service (LSASS)のサービス拒否 (DoS) の脆弱性	重要	6.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50371	Windows LUA File Virtualization Filter Driverの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58544	Windows Management Servicesの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50404	Windows Mediaの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50358	Windows Mediaの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50336	Windows Mediaの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50398	Windows Mediaの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50414	Windows Mediaの特権昇格の脆弱性	重要	7.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50379	Windows Mediaの特権昇格の脆弱性	重要	7.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50433	Windows Mediaの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50676	Windows Mediaの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50677	Windows Mediaの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-34349	Windows Mediaの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-50394	Windows Mediaの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50415	Windows Mediaの情報漏洩の脆弱性	重要	5.3	いいえ	いいえ	情報漏洩
CVE-2026-57083	Windows Media Photo Codecの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-54115	Windows Message Queuing (MSMQ)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50447	Windows Message Queuing Service (MSMQ)のリモートコード実行の脆弱性	重要	9.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50505	Windows Message Queuing Service (MSMQ)のリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50342	Windows MIDI Service Moduleの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56183	Windows MIDI Service Moduleの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56187	Windows MIDI Service Moduleの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58635	Windows Narrator Brailleの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50500	Windows Netlogonの特権昇格の脆弱性	重要	7.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50476	Windows Network Connections Serviceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50450	Windows Network Connections Serviceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56650	Windows Network File Systemの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56649	Windows Network File Systemのリモートコード実行の脆弱性	重要	5.9	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50470	Windows Network Policy Server SNMPの情報漏洩の脆弱性	重要	7.5	いいえ	いいえ	情報漏洩
CVE-2026-50496	Windows Network Policy Server SNMPの情報漏洩の脆弱性	重要	7.5	いいえ	いいえ	情報漏洩
CVE-2026-56194	Windows NFS Serverの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56648	Windows NFS Serverの特権昇格の脆弱性	重要	7.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50337	Windows Notificationの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49789	Windows NTFSの特権昇格の脆弱性	重要	7.3	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50412	Windows NTFSの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50422	Windows NTFSの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-50672	Windows NTFSの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56175	Windows NTFSの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56182	Windows NTFSの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50341	Windows NTFSの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-58640	Windows NTFSのリモートコード実行の脆弱性	重要	7.3	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49184	Windows NTFSのリモートコード実行の脆弱性	重要	8.4	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49797	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50308	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50386	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50309	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50313	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50388	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50448	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50471	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50461	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50417	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50482	Windows NTFSのリモートコード実行の脆弱性	重要	7.3	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50494	Windows NTFSのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50344	Windows OLEの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50686	Windows OLEのリモートコード実行の脆弱性	重要	8.1	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50335	Windows Operating Systemsの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50317	Windows Operating Systemsの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-54987	Windows Overlay Filterの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50435	Windows Overlay Filterの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50409	Windows Overlay Filterの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-40400	Windows PowerShellのリモートコード実行の脆弱性	重要	8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49166	Windows Print Configurationの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-55004	Windows Print Configurationの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50499	Windows Print Spoolerの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50383	Windows Print Spoolerの情報漏洩の脆弱性	重要	6.1	いいえ	いいえ	情報漏洩
CVE-2026-57085	Windows Print Spoolerの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50469	Windows Projected File Systemの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50434	Windows Push Notificationの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50339	Windows Push Notificationの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50430	Windows Push Notificationの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50334	Windows Push Notificationの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-44800	Windows Push Notificationsの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50363	Windows Push Notificationsの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50431	Windows Quality of Service (QoS) Packet Schedulerの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50372	Windows Redirected Drive Buffering Systemの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50666	Windows Remote Accessの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56647	Windows Remote Access Service Infrastructureの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50330	Windows Remote Desktop Clientの特権昇格の脆弱性	重要	7.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50376	Windows Remote Desktop Clientの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-50504	Windows Remote Desktop Clientの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-58533	Windows Remote Desktop Clientの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-58535	Windows Remote Desktop Clientの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-58546	Windows Remote Desktop Clientの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-58539	Windows Remote Desktop Clientの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-55003	Windows Remote Desktop Protocol (RDP)の情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-57979	Windows Remote Desktop Protocol (RDP)の情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-50445	Windows Remote Desktop Protocol (RDP)の情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-50497	Windows Remote Desktop Protocol (RDP)の情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-54126	Windows Remote Desktop Protocol (RDP)の情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-57982	Windows Remote Desktop Protocol (RDP)の情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-50369	Windows Remote Desktop Servicesの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58626	Windows Remote Desktop Servicesのリモートコード実行の脆弱性	重要	8.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-55014	Windows Remote Help Defenseの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50318	Windows Resilient File System (ReFS)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50407	Windows Resilient File System (ReFS)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50357	Windows Resilient File System (ReFS)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50441	Windows Resilient File System (ReFS)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50668	Windows Resilient File System (ReFS)の特権昇格の脆弱性	重要	6.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54109	Windows Resilient File System (ReFS)のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49792	Windows Resilient File System (ReFS)のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49793	Windows Resilient File System (ReFS)のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50362	Windows Resilient File System (ReFS)のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50492	Windows Resilient File System (ReFS)のリモートコード実行の脆弱性	重要	6.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50501	Windows Resilient File System (ReFS)のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-58530	Windows Resilient File System (ReFS)のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-49791	Windows Routing and Remote Access Service (RRAS)の特権昇格の脆弱性	重要	7.1	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50451	Windows Routing and Remote Access Service (RRAS)の特権昇格の脆弱性	重要	7.1	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-57096	Windows Routing and Remote Access Service (RRAS)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-50323	Windows Runtimeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50452	Windows Runtimeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50348	Windows Runtimeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50345	Windows Runtimeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50322	Windows Runtimeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50340	Windows Runtimeの特権昇格の脆弱性	重要	8.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50410	Windows Runtimeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50449	Windows Runtimeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50460	Windows Runtimeの特権昇格の脆弱性	重要	8.1	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50403	Windows Runtimeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50385	Windows Runtimeの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50413	Windows Runtimeの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50457	Windows Runtimeの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50486	Windows Runtimeの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50503	Windows Runtimeの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54125	Windows Runtimeの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58527	Windows Runtimeの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50373	Windows Search Serviceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50679	Windows Search Serviceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-44806	Windows Secure Channelのサービス拒否 (DoS) の脆弱性	重要	5.3	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50681	Windows Secure Channelの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-56186	Windows Secure Channelの情報漏洩の脆弱性	重要	8.1	いいえ	いいえ	情報漏洩

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-50367	Windows Sensor Data Serviceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58619	Windows Sensor Data Serviceの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50311	Windows Serverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50328	Windows Server Update Service (WSUS)の改ざんの脆弱性	重要	7.5	いいえ	いいえ	改ざん
CVE-2026-58531	Windows SMBの特権昇格の脆弱性	重要	7.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54997	Windows SMBの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-49801	Windows SMBの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50690	Windows SMBの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-56168	Windows SMB Serverのサービス拒否 (DoS) の脆弱性	重要	6.5	いいえ	いいえ	サービス拒否 (DoS)
CVE-2026-50360	Windows SMB Serverの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-57089	Windows SMB Server Network Transport Driver (srvnet.sys)のリモートコード実行の脆弱性	重要	7.5	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50333	Windows Spaceport.sysの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50298	Windows Spaceport.sysの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49171	Windows Speech Runtimeの特権昇格の脆弱性	重要	7.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49170	Windows StateRepository API Server fileの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58526	Windows Storageの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50299	Windows Storage Spaces Directのリモートコード実行の脆弱性	重要	6.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-57968	Windows Subsystem for Linux (WSL2) Kernelの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-57973	Windows Subsystem for Linux (WSL2) Kernelの改ざんの脆弱性	重要	6.3	いいえ	いいえ	改ざん
CVE-2026-50418	Windows Systemのセキュリティ機能のバイパスの脆弱性	重要	5.1	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-50306	Windows TCP/IPの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50307	Windows TCP/IPの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49177	Windows TCP/IPの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-50669	Windows Telephony Serverの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54124	Windows Terminalのリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	リモートコード実行 (RCE)
CVE-2026-50350	Windows Trusted Runtime Interface Driverの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-50326	Windows Unified Consent Systemの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49790	Windows Universal Disk Format File System Driver (UDFS)の特権昇格の脆弱性	重要	7.3	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50498	Windows Universal Disk Format File System Driver (UDFS)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58547	Windows Universal Plug and Play (UPnP) Device Hostの特権昇格の脆弱性	重要	5.5	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49794	Windows USB Audio Class Driverの情報漏洩の脆弱性	重要	4.6	いいえ	いいえ	情報漏洩
CVE-2026-50453	Windows USB Audio Class Driverの情報漏洩の脆弱性	重要	6.1	いいえ	いいえ	情報漏洩
CVE-2026-58528	Windows USB Audio Class Driverの情報漏洩の脆弱性	重要	6.8	いいえ	いいえ	情報漏洩
CVE-2026-50321	Windows USB Driverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50479	Windows USB Hub Driverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-55000	Windows USB Print Driverの特権昇格の脆弱性	重要	6.4	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54991	Windows USB Print Driverの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54996	Windows USB Print Driverの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49802	Windows USB Print Driverの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49806	Windows USB Print Driverの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50674	Windows USB Print Driverの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49804	Windows USB Video Driverの特権昇格の脆弱性	重要	6.6	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50454	Windows User Interface Coreの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49176	Windows WalletServiceの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-49800	Windows Web Proxy Auto-Discovery Protocol (WPAD)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50480	Windows Web Proxy Auto-Discovery Protocol (WPAD)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)

CVE	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-56173	Windows WebViewの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58632	Windows Win32 Kernel Subsystemの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54107	Windows Win32kの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54986	Windows Win32kの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54112	Windows Win32kの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-54114	Windows Win32kの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50670	Windows Win32kの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50688	Windows Win32kの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50687	Windows Win32kの特権昇格の脆弱性	重要	8.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-56176	Windows Win32kの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-58628	Windows Wireless Network Managerの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-50295	Windows Zero Trust DNSのセキュリティ機能のバイパスの脆弱性	重要	5.5	いいえ	いいえ	セキュリティ機能のバイパス (SFB)
CVE-2026-50509	Wireless Wide Area Network Service (WwanSvc)の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	特権昇格 (EoP)
CVE-2026-55945	Microsoft Edge (Chromium-based)の情報漏洩の脆弱性	警告	4.2	いいえ	いいえ	情報漏洩
CVE-2026-45488	Microsoft Edge (Chromium-based)のなりすましの脆弱性	警告	5.4	いいえ	いいえ	なりすまし
CVE-2026-45489	Microsoft Edge (Chromium-based)のなりすましの脆弱性	警告	6.5	いいえ	いいえ	なりすまし
CVE-2026-55145	Outlook Copilotの改ざんの脆弱性	警告	6.3	いいえ	いいえ	改ざん
CVE-2026-56181	Windows Network Address Translation (NAT)のなりすましの脆弱性	警告	8.3	いいえ	いいえ	なりすまし
CVE-2026-58597	Microsoft Edge (Chromium-based)のなりすましの脆弱性	注意	4.3	いいえ	いいえ	なりすまし

※が付いたCVE（5件）はMicrosoftによる修正がすでに完了しており、エンドユーザによる追加対応は不要です。