Microsoft 2026年9月 セキュリティアップデート

CVE 996件 / 原文表の掲載順 | CVE番号をクリックすると、Microsoft Security Response Centerの詳細情報を開きます。

深刻度：緊急（Critical）、重要（Important）、高（High）、中（Medium）、低（Low）

* は、サードパーティが公開済みで、今回Microsoftのリリースに含められたCVEを示します。
** 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が不要なCVEを示します。
† は、脆弱性に完全に対処するため、管理者による追加の対応が必要なことを示します。

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-85880	Windows Advanced Local Procedure Call (ALPC) の特権の昇格の脆弱性	重要	7.8	なし	あり	特権昇格
CVE-2026-81963	Windows Update Stack の特権の昇格の脆弱性	重要	7.8	なし	あり	特権昇格
CVE-2026-70352 **	Azure AI Language の特権の昇格の脆弱性	緊急	10	なし	なし	特権昇格
CVE-2026-69857 **	Azure Cosmos DB のなりすましの脆弱性	緊急	8.5	なし	なし	なりすまし
CVE-2026-80098 **	Copilot Studio の特権の昇格の脆弱性	緊急	9.3	なし	なし	特権昇格
CVE-2026-73006	DirectWrite 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	リモートコード実行
CVE-2026-83941 **	Entra ID の特権の昇格の脆弱性	緊急	9.9	なし	なし	特権昇格
CVE-2026-72986	Graphic Fonts 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	リモートコード実行
CVE-2026-73018	Graphic Fonts 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	リモートコード実行
CVE-2026-73017	Graphics Kernel のリモートでコードが実行される脆弱性	緊急	7.5	なし	なし	リモートコード実行
CVE-2026-58599	HEVC Video Extensions 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	リモートコード実行
CVE-2026-72981	IP Helper のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-72983	Internet Connection Sharing (ICS) のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-83711 **	Microsoft Azure Active Directory B2C の特権の昇格の脆弱性	緊急	10	なし	なし	特権昇格
CVE-2026-62906 **	Microsoft Discovery Studio の情報漏洩の脆弱性	緊急	7.4	なし	なし	情報漏洩
CVE-2026-65772	Microsoft Dynamics 365 On-Premises 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	リモートコード実行
CVE-2026-62916 **	Microsoft Entra ID の特権の昇格の脆弱性	緊急	9.1	なし	なし	特権昇格
CVE-2026-81948	Microsoft Excel 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-81949	Microsoft Excel 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	リモートコード実行
CVE-2026-81950	Microsoft Excel 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	リモートコード実行
CVE-2026-81951	Microsoft Excel 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	リモートコード実行
CVE-2026-81953	Microsoft Excel 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	リモートコード実行
CVE-2026-81959	Microsoft Excel 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	リモートコード実行
CVE-2026-70178 **	Microsoft Fabric の特権の昇格の脆弱性	緊急	8.5	なし	なし	特権昇格
CVE-2026-73010	Microsoft Failover Cluster のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-78444	Microsoft Failover Cluster のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-78439	Microsoft Office Graphics Component 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	リモートコード実行
CVE-2026-78520	Microsoft Office Outlook の情報漏洩の脆弱性	緊急	6.5	なし	なし	情報漏洩
CVE-2026-78509	Microsoft Office Outlook のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-78519	Microsoft Office Outlook のリモートでコードが実行される脆弱性	緊急		なし	なし	リモートコード実行
CVE-2026-78525	Microsoft Office Outlook 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	リモートコード実行
CVE-2026-69678	Microsoft Office PowerPoint 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	リモートコード実行
CVE-2026-69767	Microsoft Office PowerPoint 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	リモートコード実行
CVE-2026-69797	Microsoft Office PowerPoint 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	リモートコード実行
CVE-2026-69285	Microsoft Office 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	リモートコード実行
CVE-2026-69632	Microsoft Office 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	リモートコード実行
CVE-2026-77898	Microsoft Office のリモートでコードが実行される脆弱性	緊急	7.5	なし	なし	リモートコード実行
CVE-2026-78505	Microsoft Office 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	リモートコード実行
CVE-2026-77504	Microsoft Office Word 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	リモートコード実行
CVE-2026-65669	Microsoft SQL Server の特権の昇格の脆弱性	緊急	9.6	なし	なし	特権昇格
CVE-2026-67378	Microsoft SQL Server のリモートでコードが実行される脆弱性	緊急	8.5	なし	なし	リモートコード実行
CVE-2026-67631	Microsoft SQL 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-67636	Microsoft SQL Server のリモートでコードが実行される脆弱性	緊急	8.5	なし	なし	リモートコード実行
CVE-2026-67643	Microsoft SQL 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	リモートコード実行
CVE-2026-70351	Microsoft WebP Image Extension 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	リモートコード実行
CVE-2026-69601	Microsoft Windows Media Foundation 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	リモートコード実行
CVE-2026-78510	Microsoft Word のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-81952	Microsoft Word 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	リモートコード実行
CVE-2026-65818 **	Power Automate の特権の昇格の脆弱性	緊急	8.5	なし	なし	特権昇格
CVE-2026-69649	Raw Image Extension 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	リモートコード実行
CVE-2026-66302	Skype for Business のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-69854	Spring Cloud Azure の特権の昇格の脆弱性	緊急	9	なし	なし	特権昇格
CVE-2026-81355	Virtual Hard Disk (VHD) Miniport Driver のリモートでコードが実行される脆弱性	緊急	7.5	なし	なし	リモートコード実行
CVE-2026-81352	Web Media Extensions 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	リモートコード実行
CVE-2026-69874	Windows ALPC の特権の昇格の脆弱性	緊急	8.2	なし	なし	特権昇格
CVE-2026-72958	Windows Credential Guard の特権の昇格の脆弱性	緊急	8.2	なし	なし	特権昇格
CVE-2026-69845	Windows DHCP Server のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-72979	Windows DHCP Server のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-72987	Windows DNS のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-69730	Windows DNS Server のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-69813	Windows DNS Server のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-69827	Windows DNS Server のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-69858	Windows DNS Server のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-77505	Windows DNS Server のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-72954	Windows Deployment Services のリモートでコードが実行される脆弱性	緊急	7.5	なし	なし	リモートコード実行
CVE-2026-72957	Windows Deployment Services 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-77493	Windows Graphics Component のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-81955	Windows Graphics Component 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	リモートコード実行
CVE-2026-69769	Windows HTTP Print Provider のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-69710	Windows Hello の特権の昇格の脆弱性	緊急	7.5	なし	なし	特権昇格
CVE-2026-69725	Windows Hello の特権の昇格の脆弱性	緊急	7.8	なし	なし	特権昇格
CVE-2026-69740	Windows Hello の特権の昇格の脆弱性	緊急	8.8	なし	なし	特権昇格
CVE-2026-69784	Windows Hello の特権の昇格の脆弱性	緊急	8.8	なし	なし	特権昇格
CVE-2026-69799	Windows Hello の特権の昇格の脆弱性	緊急	7.8	なし	なし	特権昇格
CVE-2026-69820	Windows Hello の特権の昇格の脆弱性	緊急	8.2	なし	なし	特権昇格
CVE-2026-69864	Windows Hello の特権の昇格の脆弱性	緊急	7.8	なし	なし	特権昇格
CVE-2026-81354	Windows Hello の特権の昇格の脆弱性	緊急	8.2	なし	なし	特権昇格
CVE-2026-72980	Windows Hello のセキュリティ機能のバイパスの脆弱性	緊急	4.4	なし	なし	セキュリティ機能のバイパス
CVE-2026-72961	Windows Hyper-V の特権の昇格の脆弱性	緊急	8.2	なし	なし	特権昇格
CVE-2026-69603	Windows Hyper-V 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	リモートコード実行
CVE-2026-80083	Windows Hyper-V 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	リモートコード実行
CVE-2026-69499	Windows Imaging Component 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	リモートコード実行
CVE-2026-69860	Windows Imaging Component 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	リモートコード実行
CVE-2026-70296	Windows Imaging Component のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-73013	Windows Imaging Component 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	リモートコード実行
CVE-2026-73023	Windows Imaging Component 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	リモートコード実行
CVE-2026-77495	Windows Imaging Component 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	リモートコード実行
CVE-2026-69676	Windows Kerberos 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	リモートコード実行
CVE-2026-69712	Windows Key Distribution Center 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	リモートコード実行
CVE-2026-70203	Windows Media Player 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-72960	Windows Media Player 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	リモートコード実行
CVE-2026-69579	Windows Message Queuing のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-72982	Windows Netlogon のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-70586	Windows Paint 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	リモートコード実行
CVE-2026-69530	Windows Reliable Multicast Transport Driver (RMCAST) のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-78449	Windows Reliable Multicast Transport Driver (RMCAST) のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-78450	Windows Reliable Multicast Transport Driver (RMCAST) のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-69518	Windows Remote Desktop 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	リモートコード実行
CVE-2026-69590	Windows Routing and Remote Access Service (RRAS) のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-69852	Windows Routing and Remote Access Service (RRAS) のリモートでコードが実行される脆弱性	緊急	7.5	なし	なし	リモートコード実行
CVE-2026-72950	Windows Routing and Remote Access Service (RRAS) 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	リモートコード実行
CVE-2026-72959	Windows Routing and Remote Access Service (RRAS) 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	リモートコード実行
CVE-2026-69501	Windows Secure Kernel Mode の特権の昇格の脆弱性	緊急	7	なし	なし	特権昇格
CVE-2026-69846	Windows Secure Kernel Mode の特権の昇格の脆弱性	緊急	8.2	なし	なし	特権昇格
CVE-2026-69906	Windows Secure Kernel Mode の特権の昇格の脆弱性	緊急	8.2	なし	なし	特権昇格
CVE-2026-83939	Windows Secure Kernel Mode の特権の昇格の脆弱性	緊急	8.2	なし	なし	特権昇格
CVE-2026-73009	Windows Secure Socket Tunneling Protocol (SSTP) のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-69595	Windows Services for NFS ONCRPC XDR Driver のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70585	Windows Services for NFS ONCRPC XDR Driver のリモートでコードが実行される脆弱性	緊急	7	なし	なし	リモートコード実行
CVE-2026-78445	Windows Services for NFS ONCRPC XDR Driver のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-69829	Windows Shell のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-72962	Windows USB Video Driver の特権の昇格の脆弱性	緊急	8.2	なし	なし	特権昇格
CVE-2026-69890	Windows Virtual Trusted Platform Module の特権の昇格の脆弱性	緊急	7.5	なし	なし	特権昇格
CVE-2026-83498	Windows Virtualization-Based Security (VBS) Enclave の特権の昇格の脆弱性	緊急	7.8	なし	なし	特権昇格
CVE-2026-83501	Windows Virtualization-Based Security (VBS) の情報漏洩の脆弱性	緊急	5.5	なし	なし	情報漏洩
CVE-2026-69805	.NET の特権の昇格の脆弱性	重要	7.5	なし	なし	特権昇格
CVE-2026-69806	.NET の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-58649	.NET の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69439	.NET and Visual Studio の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-69522	.NET and Visual Studio 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	リモートコード実行
CVE-2026-71328	.NET and Visual Studio 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	リモートコード実行
CVE-2026-57099	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69304	ASP.NET Core のサービス拒否の脆弱性	重要	5.9	なし	なし	サービス拒否
CVE-2026-62810	Active Directory Certificate Services (AD CS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69821	Active Directory Certificate Services (AD CS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69395	Active Directory Certificate Services (AD CS) の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69624	Active Directory Certificate Services (AD CS) の改ざんの脆弱性	重要	6.5	なし	なし	改ざん
CVE-2026-69359	Active Directory Domain Services の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72978	Active Directory Federation Services (AD FS) のサービス拒否の脆弱性	重要	5.9	なし	なし	サービス拒否
CVE-2026-69401	Audio Video Control Transport Protocol の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-62895	Azure Arc SQL Server Extension の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-77909	Azure CycleCloud の情報漏洩の脆弱性	重要	7.7	なし	なし	情報漏洩
CVE-2026-81349	Azure HDInsight Ambari の特権の昇格の脆弱性	重要	7.2	なし	なし	特権昇格
CVE-2026-69329	BranchCache のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69516	Connected Devices Platform Service (Cdpsvc) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-68824	Connected User Experiences and Telemetry の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-68847	Connected User Experiences and Telemetry の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69470	Connected User Experiences and Telemetry の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69625	Connected User Experiences and Telemetry の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-73014	Data Sharing Service Client の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73016	DirectWrite 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	リモートコード実行
CVE-2026-81380	GitHub Copilot and Visual Studio Code の情報漏洩の脆弱性	重要	5.3	なし	なし	情報漏洩
CVE-2026-81381	GitHub Copilot and Visual Studio Code の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69576	Graphic Fonts の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-81353	HEIF Image Extensions 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	リモートコード実行
CVE-2026-58600	HEVC Video Extensions の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69731	HID Class Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68895	Internet Storage Name Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69275	Kernel Streaming WOW Thunk Service Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69900	Kernel Streaming WOW Thunk Service Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68850	Microsoft Account の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68852	Microsoft Account の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-84003	Microsoft Authentication Library (MSAL) for Node.js のなりすましの脆弱性	重要	7.4	なし	なし	なりすまし
CVE-2026-80097	Microsoft Authenticator の特権の昇格の脆弱性	重要	8.6	なし	なし	特権昇格
CVE-2026-83948	Microsoft Azure CLI のリモートでコードが実行される脆弱性	重要	8	なし	なし	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69299	Microsoft COM for Windows の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69294	Microsoft COM for Windows の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69491	Microsoft DirectMusic のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-77908	Microsoft Dynamics 365 On-Premises 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	リモートコード実行
CVE-2026-81387	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81390	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81391	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81392	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81393	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81394	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81395	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81399	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81400	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81401	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81958	Microsoft Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81386	Microsoft Excel 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	リモートコード実行
CVE-2026-81388	Microsoft Excel 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	リモートコード実行
CVE-2026-81389	Microsoft Excel のリモートでコードが実行される脆弱性	重要	7	なし	なし	リモートコード実行
CVE-2026-81396	Microsoft Excel 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	リモートコード実行
CVE-2026-81397	Microsoft Excel 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	リモートコード実行
CVE-2026-81398	Microsoft Excel 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	リモートコード実行
CVE-2026-81947	Microsoft Excel 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	リモートコード実行
CVE-2026-81954	Microsoft Excel 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	リモートコード実行
CVE-2026-81956	Microsoft Excel 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-81957	Microsoft Excel 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	リモートコード実行
CVE-2026-81960	Microsoft Excel 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	リモートコード実行
CVE-2026-69378	Microsoft Exchange Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69380	Microsoft Exchange Server の特権の昇格の脆弱性	重要	8.1	なし	なし	特権昇格
CVE-2026-69641	Microsoft Exchange Server の特権の昇格の脆弱性	重要	9.1	なし	なし	特権昇格
CVE-2026-69382	Microsoft Exchange Server の情報漏洩の脆弱性	重要	5.9	なし	なし	情報漏洩
CVE-2026-55007	Microsoft Exchange Server のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69355	Microsoft Exchange Server 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	リモートコード実行
CVE-2026-69356	Microsoft Exchange Server のなりすましの脆弱性	重要	9.3	なし	なし	なりすまし
CVE-2026-69361	Microsoft Exchange Server のなりすましの脆弱性	重要	6.5	なし	なし	なりすまし
CVE-2026-69375	Microsoft Exchange Server の改ざんの脆弱性	重要	6.5	なし	なし	改ざん
CVE-2026-69467	Microsoft Graphics Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83990	Microsoft Graphics Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-84000	Microsoft Graphics Component 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	リモートコード実行
CVE-2026-69605	Microsoft Install Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69325	Microsoft JScript のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69438	Microsoft JScript のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69277	Microsoft Local Security Authority (LSA) Server の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69365	Microsoft Local Security Authority (LSA) Server の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69594	Microsoft Local Security Authority (LSA) Server の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69477	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	7.3	なし	なし	リモートコード実行
CVE-2026-69529	Microsoft Office Access 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	リモートコード実行
CVE-2026-69614	Microsoft Office Access 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	リモートコード実行
CVE-2026-69778	Microsoft Office Access 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-72974	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-78515	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-85875	Microsoft Office Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-78518	Microsoft Office Excel 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	リモートコード実行
CVE-2026-69626	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69739	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-80076	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-80078	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-80082	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-80087	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-80089	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-80091	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-80073	Microsoft Office Outlook の情報漏洩の脆弱性	重要		なし	なし	情報漏洩
CVE-2026-80084	Microsoft Office Outlook の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69629	Microsoft Office Outlook 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	リモートコード実行
CVE-2026-72938	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-72956	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-72975	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-72977	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-78513	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-80086	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-80081	Microsoft Office PowerPoint のリモートでコードが実行される脆弱性	重要		なし	なし	リモートコード実行
CVE-2026-69742	Microsoft Office Publisher 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	リモートコード実行
CVE-2026-81385	Microsoft Office Publisher 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69442	Microsoft Office 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	リモートコード実行
CVE-2026-78524	Microsoft Office 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	リモートコード実行
CVE-2026-69464	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-69716	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-69409	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69636	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69683	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69904	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	3.5	なし	なし	情報漏洩
CVE-2026-69268	Microsoft Office SharePoint 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	リモートコード実行
CVE-2026-69273	Microsoft Office SharePoint 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	リモートコード実行
CVE-2026-69282	Microsoft Office SharePoint 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	リモートコード実行
CVE-2026-69465	Microsoft Office SharePoint 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	リモートコード実行
CVE-2026-69724	Microsoft Office SharePoint 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	リモートコード実行
CVE-2026-69804	Microsoft Office SharePoint のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-69402	Microsoft Office SharePoint のなりすましの脆弱性	重要	7.3	なし	なし	なりすまし
CVE-2026-69417	Microsoft Office SharePoint のなりすましの脆弱性	重要	7.3	なし	なし	なりすまし
CVE-2026-69615	Microsoft Office SharePoint のなりすましの脆弱性	重要	3.5	なし	なし	なりすまし
CVE-2026-69690	Microsoft Office SharePoint のなりすましの脆弱性	重要	4.6	なし	なし	なりすまし
CVE-2026-64918	Microsoft Office のなりすましの脆弱性	重要	6.5	なし	なし	なりすまし
CVE-2026-68843	Microsoft Office Word の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69719	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69734	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-72976	Microsoft Office Word の情報漏洩の脆弱性	重要	5	なし	なし	情報漏洩
CVE-2026-77911	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-78502	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-78503	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-78506	Microsoft Office Word の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-78522	Microsoft Office Word の情報漏洩の脆弱性	重要		なし	なし	情報漏洩
CVE-2026-80079	Microsoft Office Word の情報漏洩の脆弱性	重要		なし	なし	情報漏洩
CVE-2026-80088	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-80090	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-83949	Microsoft Office Word の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83951	Microsoft Office Word の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69360	Microsoft Office Word 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	リモートコード実行
CVE-2026-69556	Microsoft Office Word 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	リモートコード実行
CVE-2026-69671	Microsoft Office Word 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	リモートコード実行
CVE-2026-69686	Microsoft Office Word 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	リモートコード実行
CVE-2026-69722	Microsoft Office Word 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	リモートコード実行
CVE-2026-69759	Microsoft Office Word 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	リモートコード実行
CVE-2026-69764	Microsoft Office Word 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	リモートコード実行
CVE-2026-72972	Microsoft Office Word 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	リモートコード実行
CVE-2026-72973	Microsoft Office Word 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	リモートコード実行
CVE-2026-77901	Microsoft Office Word 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	リモートコード実行
CVE-2026-78504	Microsoft Office Word 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	リモートコード実行
CVE-2026-78507	Microsoft Office Word 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	リモートコード実行
CVE-2026-78511	Microsoft Office Word 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	リモートコード実行
CVE-2026-78512	Microsoft Office Word 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	リモートコード実行
CVE-2026-78514	Microsoft Office Word 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-78517	Microsoft Office Word 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	リモートコード実行
CVE-2026-78521	Microsoft Office Word 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	リモートコード実行
CVE-2026-78526	Microsoft Office Word 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	リモートコード実行
CVE-2026-80080	Microsoft Office Word 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	リモートコード実行
CVE-2026-80085	Microsoft Office Word 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	リモートコード実行
CVE-2026-69397	Microsoft OpenSSH for Windows のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-77897	Microsoft Power Automate Desktop の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-62801	Microsoft PowerShell のセキュリティ機能のバイパスの脆弱性	重要	6.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-57098	Microsoft Remote Desktop App for Windows の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-67376	Microsoft SQL Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-67633	Microsoft SQL Server のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-67641	Microsoft SQL Server のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-66814	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-66818	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-66819	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-67368	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-67370	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-67381	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-67369	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-67383	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-67386	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-67389	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-67390	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-67393	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-67624	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-67629	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-67630	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-67645	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-67648	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-68776	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-68777	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-68778	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-68779	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-68780	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-68781	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-68784	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69562	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-73029	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-77488	Microsoft SQL Server の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-47297	Microsoft SQL Server のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-67373	Microsoft SQL Server 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	リモートコード実行
CVE-2026-67379	Microsoft SQL Server のリモートでコードが実行される脆弱性	重要	8.5	なし	なし	リモートコード実行
CVE-2026-67380	Microsoft SQL Server 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	リモートコード実行
CVE-2026-67384	Microsoft SQL Server 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	リモートコード実行
CVE-2026-67385	Microsoft SQL Server 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	リモートコード実行
CVE-2026-67388	Microsoft SQL Server 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	リモートコード実行
CVE-2026-67638	Microsoft SQL Server 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	リモートコード実行
CVE-2026-67639	Microsoft SQL Server 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-67642	Microsoft SQL Server 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	リモートコード実行
CVE-2026-68775	Microsoft SQL Server 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	リモートコード実行
CVE-2026-68785	Microsoft SQL Server のリモートでコードが実行される脆弱性	重要	4.9	なし	なし	リモートコード実行
CVE-2026-68786	Microsoft SQL Server 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	リモートコード実行
CVE-2026-68787	Microsoft SQL Server 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	リモートコード実行
CVE-2026-77481	Microsoft SQL Server 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	リモートコード実行
CVE-2026-77482	Microsoft SQL Server 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	リモートコード実行
CVE-2026-77484	Microsoft SQL Server 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	リモートコード実行
CVE-2026-77486	Microsoft SQL Server 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	リモートコード実行
CVE-2026-66816	Microsoft SQL Server のセキュリティ機能のバイパスの脆弱性	重要	6.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-68885	Microsoft Standard XPS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68888	Microsoft Standard XPS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68889	Microsoft Standard XPS の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-68890	Microsoft Standard XPS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68892	Microsoft Standard XPS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68897	Microsoft Standard XPS の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69269	Microsoft Standard XPS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69271	Microsoft Standard XPS の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69272	Microsoft Standard XPS の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69313	Microsoft Standard XPS の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69336	Microsoft Standard XPS の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-68881	Microsoft Standard XPS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-68891	Microsoft Standard XPS の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-69308	Microsoft Standard XPS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69345	Microsoft Standard XPS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69367	Microsoft Standard XPS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69376	Microsoft Standard XPS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69824	Microsoft Standard XPS のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-72946	Microsoft Storage Port Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-65812	Microsoft Teams for Android の情報漏洩の脆弱性	重要	6.8	なし	なし	情報漏洩
CVE-2026-69559	Microsoft Teams for Android の情報漏洩の脆弱性	重要	5.8	なし	なし	情報漏洩
CVE-2026-56198	Microsoft Trace Data Helper の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69276	Microsoft UxTheme Library (uxtheme.dll) のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69420	Microsoft VOLSNAP.SYS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69427	Microsoft VOLSNAP.SYS の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-72933	Microsoft WDAC OLE DB provider for SQL 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	リモートコード実行
CVE-2026-62706	Microsoft Windows Media Foundation 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	リモートコード実行
CVE-2026-62744	Microsoft Windows Media Foundation 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	リモートコード実行
CVE-2026-69386	Microsoft Windows Media Foundation 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	リモートコード実行
CVE-2026-69408	Microsoft Windows Media Foundation のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69511	Microsoft Windows Media Foundation 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	リモートコード実行
CVE-2026-69586	Microsoft Windows PDF のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-78451	Microsoft Windows SCSI Class System File の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-78452	Microsoft Windows SCSI Class System File の情報漏洩の脆弱性	重要	4.6	なし	なし	情報漏洩
CVE-2026-78453	Microsoft Windows SCSI Class System File の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-68896	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69305	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69322	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69585	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69600	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69608	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69911	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69507	Microsoft Windows Search Component の情報漏洩の脆弱性	重要	5.7	なし	なし	情報漏洩
CVE-2026-70145	Microsoft Windows Search Component の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69453	Microsoft Windows Search Component の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-69554	Microsoft Windows Search Component の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-69444	Microsoft Windows Speech の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69456	Microsoft Windows Speech の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69531	Microsoft Windows Speech の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-62804	Microsoft Word 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	リモートコード実行
CVE-2026-69807	PowerShell の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69303	Push Message Routing Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69819	RPC Runtime Library のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-68828	Remote Desktop Client 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	リモートコード実行
CVE-2026-69358	Remote Desktop Client のリモートでコードが実行される脆弱性	重要	7.1	なし	なし	リモートコード実行
CVE-2026-69485	Remote Desktop Client 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	リモートコード実行
CVE-2026-78463	Remote Desktop Client 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	リモートコード実行
CVE-2026-80074	Remote Desktop Client 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	リモートコード実行
CVE-2026-80077	Remote Desktop Client 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	リモートコード実行
CVE-2026-83998	Remote Desktop Client 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	リモートコード実行
CVE-2026-69292	Remote Desktop Gateway Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69338	Remote Desktop Gateway Service の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-68893	Remote Desktop Licensing Service の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69514	Remote Desktop Services のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-69525	Remote Desktop Services のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69536	Remote Desktop Services のリモートでコードが実行される脆弱性	重要	7.1	なし	なし	リモートコード実行
CVE-2026-69539	Remote Desktop Services のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-69599	Remote Desktop Services のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-69509	Role: Windows Fax Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69621	Role: Windows Fax Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-72944	Role: Windows Fax Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-66820	SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-73028	SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-77480	SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-77483	SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-77485	SQL Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-77487	SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-78456	SQL Server 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	リモートコード実行
CVE-2026-66304	Skype for Business の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-66306	Skype for Business の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-63523	Skype for Business のなりすましの脆弱性	重要	6.5	なし	なし	なりすまし
CVE-2026-66305	Skype for Business のなりすましの脆弱性	重要	7.1	なし	なし	なりすまし
CVE-2026-69642	Skype for Business のなりすましの脆弱性	重要	6.5	なし	なし	なりすまし
CVE-2026-69646	Skype for Business のなりすましの脆弱性	重要	8.3	なし	なし	なりすまし
CVE-2026-66303	Skype for Business and Lync のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-66307	Skype for Business and Lync のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-66308	Skype for Business and Lync のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-69568	Storage Spaces Controller の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69431	Telnet Client のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69384	Virtual Hard Disk (VHD) Miniport Driver のサービス拒否の脆弱性	重要	7.1	なし	なし	サービス拒否
CVE-2026-69541	Virtual Hard Disk (VHD) Miniport Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69549	Virtual Hard Disk (VHD) Miniport Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69611	Virtual Hard Disk (VHD) Miniport Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69681	Virtual Hard Disk (VHD) Miniport Driver の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-70574	Virtual Hard Disk (VHD) Miniport Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-81383	Visual Studio Code の情報漏洩の脆弱性	重要	7.4	なし	なし	情報漏洩
CVE-2026-70334	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	7.8	なし	なし	セキュリティ機能のバイパス
CVE-2026-78461	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	7.4	なし	なし	セキュリティ機能のバイパス
CVE-2026-78462	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	なし	なし	セキュリティ機能のバイパス
CVE-2026-81356	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	8.2	なし	なし	セキュリティ機能のバイパス
CVE-2026-81357	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	8.2	なし	なし	セキュリティ機能のバイパス
CVE-2026-81376	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	9.6	なし	なし	セキュリティ機能のバイパス
CVE-2026-81378	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	8.2	なし	なし	セキュリティ機能のバイパス
CVE-2026-81379	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	8.2	なし	なし	セキュリティ機能のバイパス
CVE-2026-81377	Visual Studio Code の改ざんの脆弱性	重要	6.5	なし	なし	改ざん
CVE-2026-77906	Visual Studio 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	リモートコード実行
CVE-2026-77907	Visual Studio 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	リモートコード実行
CVE-2026-69407	Volume Manager Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69418	Volume Manager Driver の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69432	Volume Manager Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-72985	Volume Shadow Copy の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-69609	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69808	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69832	Win32k の情報漏洩の脆弱性	重要	5.6	なし	なし	情報漏洩
CVE-2026-69853	Win32k の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-70290	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70565	Windows AF_UNIX Socket Provider の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69834	Windows ALPC の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69654	Windows Accounts Control の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69816	Windows Accounts Control の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-62762	Windows Active Directory Domain Services のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-69809	Windows Active Directory Domain Services のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-62813	Windows Active Directory Domain Services のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-69524	Windows Active Directory Domain Services のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69546	Windows Active Directory Domain Services のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-50349	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70342	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	8.1	なし	なし	特権昇格
CVE-2026-69311	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69394	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69447	Windows Audio Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69540	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69604	Windows Audio Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69692	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69801	Windows Audio Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70562	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-73005	Windows Authentication Methods の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-73004	Windows Autopilot の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-68825	Windows Bind Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69293	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69298	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69323	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69352	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69476	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69489	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69580	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69583	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69589	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69593	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69727	Windows Biometric Service の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69738	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69773	Windows Biometric Service の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69787	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69826	Windows Biometric Service の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-70572	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70573	Windows Biometric Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70581	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-72941	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72988	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72990	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72991	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72992	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72993	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72994	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72995	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72996	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72997	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73000	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73001	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73002	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73007	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73011	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73015	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73020	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73021	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73026	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-77489	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-78447	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-78448	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83954	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83955	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83967	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83968	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83969	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83970	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83971	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83972	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83973	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83974	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83975	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83976	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83977	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83978	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83979	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83980	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83981	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83982	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83983	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83985	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83986	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83987	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83988	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-73008	Windows Biometric Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69458	Windows BitLocker の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69449	Windows BitLocker のリモートでコードが実行される脆弱性	重要	6.7	なし	なし	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69817	Windows Bluetooth Port Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-68849	Windows Bluetooth Port Driver の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-69388	Windows Bluetooth Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69398	Windows Bluetooth Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69448	Windows Bluetooth Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69889	Windows Bluetooth Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-77892	Windows Boot Manager の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-69735	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69391	Windows Broker Infrastructure Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69283	Windows CD-ROM Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69561	Windows CD-ROM Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-78454	Windows CD-ROM Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-78508	Windows CD-ROM Driver の情報漏洩の脆弱性	重要	4.6	なし	なし	情報漏洩
CVE-2026-69542	Windows Camera Frame Server Monitor の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69279	Windows Cloud Files Mini Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-80093	Windows Cloud Files Mini Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83991	Windows Cloud Files Mini Filter Driver の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-69445	Windows Compressed Folder の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70019	Windows Compressed Folder の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69496	Windows Compressed Folder のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69267	Windows Connected User Experiences and Telemetry の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69771	Windows Container Manager Service のセキュリティ機能のバイパスの脆弱性	重要	4.7	なし	なし	セキュリティ機能のバイパス
CVE-2026-70583	Windows Core Messaging の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70584	Windows Core Messaging の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70578	Windows Credential Guard の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69790	Windows Credential Providers の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69814	Windows Credential Providers の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69729	Windows Credential Providers 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	リモートコード実行
CVE-2026-69284	Windows DCOM Server の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69781	Windows DHCP Client のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-69777	Windows DHCP Client の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69342	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69405	Windows DHCP Server のサービス拒否の脆弱性	重要	5.7	なし	なし	サービス拒否
CVE-2026-69416	Windows DHCP Server のサービス拒否の脆弱性	重要	5.7	なし	なし	サービス拒否
CVE-2026-69497	Windows DHCP Server のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-69637	Windows DHCP Server のサービス拒否の脆弱性	重要	5.7	なし	なし	サービス拒否
CVE-2026-69679	Windows DHCP Server のサービス拒否の脆弱性	重要	5.7	なし	なし	サービス拒否
CVE-2026-70065	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-77494	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-77498	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-77499	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-77501	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-77502	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-77886	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-77888	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-77889	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-77890	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-77893	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-77895	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69415	Windows DHCP Server の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-69297	Windows DHCP Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69803	Windows DHCP Server の情報漏洩の脆弱性	重要	5.9	なし	なし	情報漏洩
CVE-2026-69929	Windows DHCP Server の情報漏洩の脆弱性	重要	5.9	なし	なし	情報漏洩
CVE-2026-69930	Windows DHCP Server の情報漏洩の脆弱性	重要	5.9	なし	なし	情報漏洩
CVE-2026-70124	Windows DHCP Server の情報漏洩の脆弱性	重要	5.9	なし	なし	情報漏洩
CVE-2026-69266	Windows DHCP Server 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	リモートコード実行
CVE-2026-69412	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	8	なし	なし	リモートコード実行
CVE-2026-69510	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69547	Windows DHCP Server 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	リモートコード実行
CVE-2026-69620	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69847	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	8	なし	なし	リモートコード実行
CVE-2026-69876	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	8	なし	なし	リモートコード実行
CVE-2026-69878	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	6.4	なし	なし	リモートコード実行
CVE-2026-77887	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	6.4	なし	なし	リモートコード実行
CVE-2026-77891	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	6.4	なし	なし	リモートコード実行
CVE-2026-69631	Windows DNS のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70091	Windows DNS のサービス拒否の脆弱性	重要	5.9	なし	なし	サービス拒否
CVE-2026-69310	Windows DNS の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-72948	Windows DNS の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-69369	Windows DNS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69672	Windows DNS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-78523	Windows DNS Server のサービス拒否の脆弱性	重要	5.9	なし	なし	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69551	Windows DNS Server 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	リモートコード実行
CVE-2026-69782	Windows DNS Server のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69989	Windows DNS Server のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-72928	Windows DNS Server のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-69680	Windows DNS のなりすましの脆弱性	重要	8.1	なし	なし	なりすまし
CVE-2026-69775	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-70568	Windows Defender Firewall Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-68831	Windows Defender Firewall Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69607	Windows Deployment Services のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-72943	Windows Deployment Services のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-69314	Windows Device Association Broker Service の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69693	Windows Device Association Broker Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69296	Windows Device Association Service の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69478	Windows Device Association Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69488	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69574	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69581	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69711	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69714	Windows Device Association Service の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69791	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69866	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-77500	Windows Device Association Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83940	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69443	Windows Device Health Attestation (DHA) の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69472	Windows Devices Human Interface の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69715	Windows Direct Show のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-70567	Windows Display Enhancement Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-78446	Windows Distributed File System (DFS) のサービス拒否の脆弱性	重要	5.3	なし	なし	サービス拒否
CVE-2026-69424	Windows Distributed File System (DFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69430	Windows Embedded Mode Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69688	Windows Encrypting File System (EFS) の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69841	Windows Encrypting File System (EFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69794	Windows Encrypting File System (EFS) の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69481	Windows Enterprise App Management の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69907	Windows Enterprise App Management の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68894	Windows Error Reporting の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69362	Windows Error Reporting の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69433	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69436	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69450	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69462	Windows Error Reporting の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69513	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69612	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69896	Windows Error Reporting の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83996	Windows Error Reporting の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-69684	Windows Error Reporting の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69482	Windows Error Reporting の改ざんの脆弱性	重要	7.1	なし	なし	改ざん
CVE-2026-69493	Windows Event Logging Service のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69494	Windows Event Logging Service 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	リモートコード実行
CVE-2026-69495	Windows Event Logging Service 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	リモートコード実行
CVE-2026-71338	Windows Failover Cluster の特権の昇格の脆弱性	重要	6.4	なし	なし	特権昇格
CVE-2026-72989	Windows Failover Cluster の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-68878	Windows Fast FAT Driver の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69347	Windows Fast FAT Driver のリモートでコードが実行される脆弱性	重要	7.4	なし	なし	リモートコード実行
CVE-2026-68837	Windows File History Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-71340	Windows File History Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-72947	Windows File History Service の特権の昇格の脆弱性	重要	6.4	なし	なし	特権昇格
CVE-2026-77491	Windows GDI の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-68827	Windows GDI+ の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69288	Windows GDI+ の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69717	Windows Group Policy の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69623	Windows HTTP Print Provider のリモートでコードが実行される脆弱性	重要	8	なし	なし	リモートコード実行
CVE-2026-69597	Windows HTTP.sys の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69682	Windows Host Guardian Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69553	Windows Hyper-V の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69910	Windows Hyper-V のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69694	Windows IP Address Management (IPAM) Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69341	Windows Image Acquisition の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69500	Windows Image Acquisition の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69613	Windows Image Acquisition の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69483	Windows Image Acquisition の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-69318	Windows Imaging Component の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83992	Windows Imaging Component 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	リモートコード実行
CVE-2026-62694	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69441	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-71339	Windows Installer の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-72929	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-77894	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-72926	Windows Internet Connection Sharing (ICS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-72964	Windows Internet Connection Sharing (ICS) の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-69587	Windows Internet Key Exchange (IKE) Extension のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69881	Windows Internet Key Exchange (IKE) Extension のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69429	Windows Internet Key Exchange (IKE) Protocol Extensions のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-69744	Windows Kerberos のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69760	Windows Kerberos のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69685	Windows Kerberos の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69822	Windows Kerberos の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68846	Windows Kernel の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-68884	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69366	Windows Kernel の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69466	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69473	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69578	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83942	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85360	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69406	Windows Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69723	Windows Kernel の情報漏洩の脆弱性	重要	5.7	なし	なし	情報漏洩
CVE-2026-69669	Windows Kernel のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69421	Windows Kernel-Mode Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-84001	Windows Key Distribution Center のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69428	Windows LDAP - Lightweight Directory Access Protocol のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69281	Windows License Manager の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69315	Windows License Manager の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69732	Windows Link Layer Topology Discovery Protocol のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69440	Windows MIDI Service Module の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69508	Windows MIDI Service Module の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69720	Windows MIDI Service Module の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-78464	Windows MIDI Service Module の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-68842	Windows MIDI Service Module の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69339	Windows MIDI Service Module の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69451	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-70582	Windows Management Instrumentation の特権の昇格の脆弱性	重要	6.4	なし	なし	特権昇格
CVE-2026-77905	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69349	Windows Management Instrumentation の情報漏洩の脆弱性	重要	5.7	なし	なし	情報漏洩
CVE-2026-73012	Windows Management Services の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-69891	Windows Media の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69645	Windows Message Queuing の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-68887	Windows Message Queuing Queue Manager のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-72932	Windows Message Queuing Queue Manager の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-83997	Windows Message Queuing のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70579	Windows Mobile Broadband の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-69377	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69460	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-70577	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-73003	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-73022	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69674	Windows Modern Device Management (MDM) 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	セキュリティ機能のバイパス
CVE-2026-72963	Windows Modern Execution Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69357	Windows NDIS の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69396	Windows NDIS の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-71334	Windows NFS Portmapper の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68832	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68834	Windows NTFS の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-68838	Windows NTFS の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-68841	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69265	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69312	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69332	Windows NTFS の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69340	Windows NTFS の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69379	Windows NTFS の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69505	Windows NTFS の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69532	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69567	Windows NTFS の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69875	Windows NTFS の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-72935	Windows NTFS の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-77503	Windows NTFS の特権の昇格の脆弱性	重要	8.4	なし	なし	特権昇格
CVE-2026-83995	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68851	Windows NTFS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69504	Windows NTFS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69591	Windows NTFS の情報漏洩の脆弱性	重要	5.7	なし	なし	情報漏洩
CVE-2026-68833	Windows NTFS のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	リモートコード実行
CVE-2026-68875	Windows NTFS 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	リモートコード実行
CVE-2026-69461	Windows NTFS 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	リモートコード実行
CVE-2026-69463	Windows NTFS のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69479	Windows NTFS のリモートでコードが実行される脆弱性	重要	8.4	なし	なし	リモートコード実行
CVE-2026-69566	Windows NTFS のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	リモートコード実行
CVE-2026-69638	Windows NTFS のリモートでコードが実行される脆弱性	重要	8.4	なし	なし	リモートコード実行
CVE-2026-69709	Windows NTFS 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	リモートコード実行
CVE-2026-71329	Windows NTFS のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	リモートコード実行
CVE-2026-69425	Windows NTFS の改ざんの脆弱性	重要	4.7	なし	なし	改ざん
CVE-2026-62759	Windows Netlogon のなりすましの脆弱性	重要	7.5	なし	なし	なりすまし
CVE-2026-72967	Windows Network Connection Broker の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68886	Windows Network Connection Broker の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69372	Windows Network File System のサービス拒否の脆弱性	重要	5.7	なし	なし	サービス拒否
CVE-2026-69772	Windows Network File System 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	リモートコード実行
CVE-2026-69648	Windows Notification の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-78441	Windows OLE DB の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-78442	Windows OLE DB 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69564	Windows Online Certificate Status Protocol (OCSP) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69350	Windows Overlay Filter の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-69368	Windows Overlay Filter の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69371	Windows Overlay Filter の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69373	Windows Overlay Filter の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-69316	Windows Overlay Filter の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-69343	Windows Overlay Filter の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69474	Windows Overlay Filter の情報漏洩の脆弱性	重要	4.8	なし	なし	情報漏洩
CVE-2026-69480	Windows Partition Management Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69492	Windows Partition Management Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-71341	Windows Partition Management Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69324	Windows Performance Monitor の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69459	Windows Power Dependency Coordinator の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69321	Windows Power Dependency Coordinator の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-69569	Windows Print Spooler Components のサービス拒否の脆弱性	重要	5.7	なし	なし	サービス拒否
CVE-2026-68835	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-68848	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69309	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69346	Windows Print Spooler Components の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69364	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69838	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69921	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70564	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69344	Windows Print Spooler Components の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69552	Windows Print Spooler Components の情報漏洩の脆弱性	重要	5.7	なし	なし	情報漏洩
CVE-2026-85877	Windows Print Spooler 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	リモートコード実行
CVE-2026-69602	Windows PrintWorkflowUserSvc の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-68845	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68876	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69534	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69563	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-68873	Windows Program Compatibility Assistant Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-68874	Windows Program Compatibility Assistant Service の情報漏洩の脆弱性	重要	5.7	なし	なし	情報漏洩
CVE-2026-62697	Windows Push Notifications の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69280	Windows Push Notifications の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69300	Windows Push Notifications の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69548	Windows RNDIS の情報漏洩の脆弱性	重要	4.6	なし	なし	情報漏洩
CVE-2026-69768	Windows RNDIS のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69337	Windows Registry の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69331	Windows Remote Access Connection Manager の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69455	Windows Remote Access Connection Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-71333	Windows Remote Access Connection Manager の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-71342	Windows Remote Access Connection Manager の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-71343	Windows Remote Access Connection Manager 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	リモートコード実行
CVE-2026-71352	Windows Remote Access Connection Manager 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	リモートコード実行
CVE-2026-72966	Windows Remote Access Connection Manager の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-77896	Windows Remote Desktop Client のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69317	Windows Remote Desktop Client の情報漏洩の脆弱性	重要	5.7	なし	なし	情報漏洩
CVE-2026-69627	Windows Remote Desktop Licensing Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70587	Windows Remote Desktop Protocol の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-69287	Windows Remote Desktop Services の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69475	Windows Remote Desktop Services の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-80096	Windows Remote Desktop Services の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-69616	Windows Remote Desktop Services の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83999	Windows Resilient File System (ReFS) Deduplication Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69617	Windows Resilient File System (ReFS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83952	Windows Resilient File System (ReFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-72939	Windows Routing and Remote Access Service (RRAS) のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-71351	Windows Routing and Remote Access Service (RRAS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-71353	Windows Routing and Remote Access Service (RRAS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70570	Windows Routing and Remote Access Service (RRAS) のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-69544	Windows SMB Client の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69572	Windows SMB Client の情報漏洩の脆弱性	重要	5.7	なし	なし	情報漏洩
CVE-2026-69618	Windows SMB Client の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-72936	Windows SMB Client のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69374	Windows SMB Server のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-69403	Windows SMB Server の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-72949	Windows SMB Server Network Transport Driver (srvnet.sys) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70575	Windows Schannel のサービス拒否の脆弱性	重要	5.3	なし	なし	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-72940	Windows Schannel 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	リモートコード実行
CVE-2026-69713	Windows Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	4.4	なし	なし	セキュリティ機能のバイパス
CVE-2026-72931	Windows Secure Socket Tunneling Protocol (SSTP) のサービス拒否の脆弱性	重要	4.7	なし	なし	サービス拒否
CVE-2026-71332	Windows Secure Socket Tunneling Protocol (SSTP) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-72930	Windows Secure Socket Tunneling Protocol (SSTP) のリモートでコードが実行される脆弱性	重要	7	なし	なし	リモートコード実行
CVE-2026-77899	Windows Security Center の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-78457	Windows Security Health Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-56177	Windows Server の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83989	Windows Services for NFS ONCRPC XDR Driver のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-73024	Windows Services for NFS ONCRPC XDR Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-71330	Windows Services for NFS ONCRPC XDR Driver の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-69289	Windows Setup Files Cleanup の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69383	Windows Shell の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69392	Windows Shell の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69528	Windows Shell の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69606	Windows Shell の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70563	Windows Shell のなりすましの脆弱性	重要	8.1	なし	なし	なりすまし
CVE-2026-69785	Windows Smart Card の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69512	Windows Spaceport.sys の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69535	Windows Spaceport.sys の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69643	Windows Spaceport.sys の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69691	Windows Spaceport.sys の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70569	Windows Spaceport.sys の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69390	Windows Spaceport.sys の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69393	Windows Spaceport.sys の情報漏洩の脆弱性	重要	5.7	なし	なし	情報漏洩
CVE-2026-69741	Windows Spaceport.sys の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69770	Windows Spaceport.sys の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69895	Windows Spaceport.sys の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-72942	Windows Spaceport.sys の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69538	Windows Spaceport.sys 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	リモートコード実行
CVE-2026-71345	Windows Spaceport.sys 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	リモートコード実行
CVE-2026-71348	Windows Spaceport.sys のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	リモートコード実行
CVE-2026-71349	Windows Spaceport.sys のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	リモートコード実行
CVE-2026-71350	Windows Spaceport.sys のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	リモートコード実行
CVE-2026-72952	Windows Spaceport.sys のリモートでコードが実行される脆弱性	重要	7	なし	なし	リモートコード実行
CVE-2026-69328	Windows Storage の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-78516	Windows Storage の情報漏洩の脆弱性	重要	4.3	なし	なし	情報漏洩
CVE-2026-69389	Windows Storage Management Provider の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-71337	Windows Storage Management Provider の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69381	Windows Storage Port Driver の情報漏洩の脆弱性	重要	4.6	なし	なし	情報漏洩
CVE-2026-72937	Windows Storage Port Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-77492	Windows Storage Port Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69290	Windows Storage Spaces Controller の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69575	Windows Storage Spaces Controller の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-68844	Windows Storage Spaces Controller 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	リモートコード実行
CVE-2026-68877	Windows Storage Spaces Controller 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	リモートコード実行
CVE-2026-69588	Windows TCP/IP のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69385	Windows TCP/IP の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69404	Windows TCP/IP の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69757	Windows TCP/IP の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69761	Windows TCP/IP の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69793	Windows TCP/IP のセキュリティ機能のバイパスの脆弱性	重要	7.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-72945	Windows Task Scheduler の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69353	Windows Text Shaping の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69786	Windows Text Shaping のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69434	Windows URL Moniker 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	リモートコード実行
CVE-2026-73019	Windows URL Moniker 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	セキュリティ機能のバイパス
CVE-2026-69286	Windows USB Audio Class Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69270	Windows USB Audio Class driver (usbaudio.sys) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69307	Windows USB Audio Class driver (usbaudio.sys) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69413	Windows USB Audio Class driver (usbaudio.sys) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69469	Windows USB Audio Class driver (usbaudio.sys) の特権の昇格の脆弱性	重要	6.6	なし	なし	特権昇格
CVE-2026-69571	Windows USB Audio Class driver (usbaudio.sys) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69687	Windows USB Audio Class driver (usbaudio.sys) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69707	Windows USB Audio Class driver (usbaudio.sys) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69859	Windows USB Audio Class driver (usbaudio.sys) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-68840	Windows USB Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69295	Windows USB Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69503	Windows USB Driver の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-72953	Windows USB Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69457	Windows USB Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-72999	Windows USB Hub Driver の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69490	Windows USB Mass Storage Class Driver の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-69527	Windows USB Mass Storage Class Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-68839	Windows USB Mass Storage Class Driver のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69319	Windows USB Video Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69422	Windows USB Video Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69423	Windows USB Video Driver の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69584	Windows USB Video Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69573	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69592	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69758	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-68830	Windows Universal Plug and Play (UPnP) Device Host の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69351	Windows Universal Plug and Play (UPnP) Device Host の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-56172	Windows VHD miniport driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69426	Windows VOLSNAP.SYS 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	リモートコード実行
CVE-2026-69468	Windows Volume Manager Extension Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69582	Windows Volume Manager Extension Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-77904	Windows Volume Manager Extension Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69291	Windows Volume Manager Extension Driver 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	リモートコード実行
CVE-2026-69334	Windows Volume Manager Extension Driver 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	リモートコード実行
CVE-2026-69708	Windows Web Platform Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-72965	Windows WebClient Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69792	Windows Win32K のセキュリティ機能のバイパスの脆弱性	重要	4.7	なし	なし	セキュリティ機能のバイパス
CVE-2026-68880	Windows Win32k の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69274	Windows Win32k の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69301	Windows Win32k の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69333	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69335	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69348	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69410	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69498	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69610	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69630	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69652	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69689	Windows Win32k の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69706	Windows Win32k の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69762	Windows Win32k の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-69779	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69818	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69844	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70283	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70289	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69517	Windows Wireless Networking の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69862	Windows Wireless Wide Area Network Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69560	Windows Work Folder Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-71336	Windows Work Folder Service 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	リモートコード実行
CVE-2026-80075	Windows Work Folders の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69619	Windows exFAT File System の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-68898	Windows iSCSI のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69598	Windows iSCSI 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	リモートコード実行
CVE-2026-69628	Windows iSCSI 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	リモートコード実行
CVE-2026-73025	Windows iSCSI のセキュリティ機能のバイパスの脆弱性	重要	9.8	なし	なし	セキュリティ機能のバイパス
CVE-2026-69839	Windows iSCSI Target Service のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-72927	Winsock の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-58611	Xbox Gaming Services の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-78455	Xbox の情報漏洩の脆弱性	重要	4.3	なし	なし	情報漏洩
CVE-2026-84353 *	Chromium: CVE-2026-84353 Shared Tab Groups における解放済みメモリの使用	緊急	N/A	なし	なし	リモートコード実行
CVE-2026-84324 *	Chromium: CVE-2026-84324 Proxy における解放済みメモリの使用	高	N/A	なし	なし	リモートコード実行
CVE-2026-84325 *	Chromium: CVE-2026-84325 DataTransfer における入力検証の不備	高	N/A	なし	なし	リモートコード実行
CVE-2026-84326 *	Chromium: CVE-2026-84326 V8 における未初期化のリソース	高	N/A	なし	なし	リモートコード実行
CVE-2026-84359 *	Chromium: CVE-2026-84359 Skia における情報漏洩	高	N/A	なし	なし	情報漏洩
CVE-2026-84357 *	Chromium: CVE-2026-84357 Omnibox における入力検証の不備	高	N/A	なし	なし	リモートコード実行
CVE-2026-84349 *	Chromium: CVE-2026-84349 Browser における解放済みメモリの使用	高	N/A	なし	なし	リモートコード実行
CVE-2026-84351 *	Chromium: CVE-2026-84351 GPU におけるバッファオーバーフロー	高	N/A	なし	なし	リモートコード実行
CVE-2026-84354 *	Chromium: CVE-2026-84354 FileSystem における不適切な認可	高	N/A	なし	なし	リモートコード実行
CVE-2026-84323 *	Chromium: CVE-2026-84323 FileSystem における認可の欠如	中	N/A	なし	なし	リモートコード実行
CVE-2026-84328 *	Chromium: CVE-2026-84328 FileSystem における認可の欠如	中	N/A	なし	なし	リモートコード実行
CVE-2026-84332 *	Chromium: CVE-2026-84332 SiteSettings における不適切な認可	中	N/A	なし	なし	リモートコード実行
CVE-2026-84334 *	Chromium: CVE-2026-84334 Chromoting における不適切な認可	中	N/A	なし	なし	特権昇格
CVE-2026-84335 *	Chromium: CVE-2026-84335 TabStrip における不適切な認可	中	N/A	なし	なし	特権昇格
CVE-2026-84347 *	Chromium: CVE-2026-84347 WebRTC における解放済みメモリの使用	中	N/A	なし	なし	リモートコード実行
CVE-2026-84348 *	Chromium: CVE-2026-84348 MediaCapture における情報漏洩	中	N/A	なし	なし	情報漏洩
CVE-2026-84355 *	Chromium: CVE-2026-84355 Navigation における不適切な認可	中	N/A	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-84358 *	Chromium: CVE-2026-84358 Downloads における不適切な特権管理	中	N/A	なし	なし	特権昇格
CVE-2026-84327 *	Chromium: CVE-2026-84327 Autofill における不適切な認可	低	N/A	なし	なし	なりすまし
CVE-2026-84329 *	Chromium: CVE-2026-84329 CredentialProvider における代理の混乱 (Confused Deputy)	低	N/A	なし	なし	特権昇格
CVE-2026-84331 *	Chromium: CVE-2026-84331 Actor における不適切な認可	低	N/A	なし	なし	セキュリティ機能のバイパス
CVE-2026-84350 *	Chromium: CVE-2026-84350 TabStrip における解放済みメモリの使用	低	N/A	なし	なし	リモートコード実行
CVE-2026-84356 *	Chromium: CVE-2026-84356 FullScreen におけるユーザインターフェースの誤表示	低	N/A	なし	なし	なりすまし

出典：Zero Day Initiative - The September 2026 Security Update Review