Microsoft 2026年8月セキュリティアップデート一覧

420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-2026-68820	Windows Ancillary Function Driver for WinSockの特権昇格の脆弱性	重要	7	いいえ	はい	特権昇格（EoP）
CVE-2026-62832	Windows User Profile Serviceの特権昇格の脆弱性	重要	7.8	はい	いいえ	特権昇格（EoP）
CVE-2026-49163 ※※	Application Insights Profiler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-2026-50481 ※※	Azure Active Directory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-2026-68823 ※※	Azure Confidential Ledgerのリモートコード実行の脆弱性	緊急	9.1	いいえ	いいえ	リモートコード実行（RCE）
CVE-2026-62869 ※※	Azure Entra IDのなりすましの脆弱性	緊急	8.8	いいえ	いいえ	なりすまし
CVE-2026-56161 ※※	Azure Logic Appsの情報漏洩の脆弱性	緊急	9.6	いいえ	いいえ	情報漏洩
CVE-2026-50515 ※※	Azure Service Busのリモートコード実行の脆弱性	緊急	9.9	いいえ	いいえ	リモートコード実行（RCE）
CVE-2026-56162 ※※	Azure SQL Databaseの特権昇格の脆弱性	緊急	10	いいえ	いいえ	特権昇格（EoP）
CVE-2026-63522 ※※	Azure SQL Database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-2026-62836 ※※	Azure SQL Managed Instanceの特権昇格の脆弱性	緊急	8.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-62830 ※※	Azure SRE Agent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-2026-62873 ※※	Microsoft 365 Admin Centerの特権昇格の脆弱性	緊急	9.8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-50516 ※※	Microsoft Azure Kubernetes Serviceの特権昇格の脆弱性	緊急	9.4	いいえ	いいえ	特権昇格（EoP）
CVE-2026-59115 ※※	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-2026-68794	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-2026-68804	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-2026-68816	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-2026-62911	Microsoft Exchange Serverの特権昇格の脆弱性	緊急	8	いいえ	いいえ	特権昇格（EoP）
CVE-2026-63513	Microsoft Office Graphics Component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-2026-63519	Microsoft Office Graphics Component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-2026-63526	Microsoft Office Graphics Component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-2026-65664	Microsoft Office Graphics Component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-2026-66807	Microsoft Office Graphics Component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-2026-63515	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-2026-63532	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-2026-64898	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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-64903	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-2026-64909	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-2026-64910	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-2026-64911	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-2026-65657	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-2026-70130	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-2026-70332 ※※	Microsoft Office SharePoint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-2026-63518	Microsoft Office 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-2026-63525	Microsoft Office 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-2026-64907	Microsoft Office 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-2026-63508 ※※	Microsoft Planetary Computer Proの特権昇格の脆弱性	緊急	10	いいえ	いいえ	特権昇格（EoP）
CVE-2026-59118 ※※	Microsoft Power Apps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-2026-65668 ※※	Microsoft Purview eDiscovery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-2026-62815	Microsoft QUIC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-2026-62827	Microsoft SharePoint Server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-2026-64921	Microsoft SharePoint Server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-2026-65665	Microsoft SharePoint 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-2026-62896 ※※	Microsoft Teamsの特権昇格の脆弱性	緊急	9.6	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65667 ※※	Microsoft Teamsの特権昇格の脆弱性	緊急	10	いいえ	いいえ	特権昇格（EoP）
CVE-2026-62918 ※※	Microsoft Teamsのなりすましの脆弱性	緊急	7.5	いいえ	いいえ	なりすまし
CVE-2026-62824	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-2026-62818	Windows Active Directory Certificate Services (AD CS)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-2026-62893	Windows Deployment Services TFTP 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-2026-66802	Windows Device Health Attestation (DHA)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-2026-71331	Windows Device Health Attestation (DHA)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-2026-62823	Windows DHCP 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-2026-62817	Windows DNS 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-2026-62820	Windows DNS Server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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-62878	Windows DNS 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-2026-65789	Windows DNS Server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-2026-62890	Windows GDI+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-2026-62822	Windows GDI+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-2026-65791	Windows iSCSI Target 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-2026-66799	Windows Key Guard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-2026-62816	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-2026-62819	Windows Routing and Remote Access Service (RRAS)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-2026-62889	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-2026-70354	.NET Core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-2026-62901	.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-2026-58641	.NET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-2026-62871	.NET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-2026-62886	.NET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-2026-62909	.NET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-2026-62872	.NET Framework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-2026-65810	.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-2026-62897	.NET Frameworkのリモートコード実行の脆弱性	重要	7	いいえ	いいえ	リモートコード実行（RCE）
CVE-2026-62900	.NETの情報漏洩の脆弱性	重要	5.9	いいえ	いいえ	情報漏洩
CVE-2026-62902	.NETの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-62899	.NETのセキュリティ機能のバイパスの脆弱性	重要	5.9	いいえ	いいえ	セキュリティ機能のバイパス（SFB）
CVE-2026-65777	Active Directoryのセキュリティ機能のバイパスの脆弱性	重要	5.3	いいえ	いいえ	セキュリティ機能のバイパス（SFB）
CVE-2026-59130	AMD Zenの情報漏洩の脆弱性	重要	5.6	いいえ	いいえ	情報漏洩
CVE-2026-59131	AMD Zenの情報漏洩の脆弱性	重要	5.6	いいえ	いいえ	情報漏洩
CVE-2026-62898	Microsoft QUICの情報漏洩の脆弱性	重要	7.5	いいえ	いいえ	情報漏洩
CVE-2026-61357	Application Information 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-2026-70340	Azure CycleCloud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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-65806	Azure CycleCloudの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-47299	Azure Monitor Agentの特権昇格の脆弱性	重要	7.2	いいえ	いいえ	特権昇格（EoP）
CVE-2026-57104	Azure Storage Explorer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-2026-62892	Capability Access Management Service (camsvc)の特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65675	CoPilot Chat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-2026-65786	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-2026-65787	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-2026-65788	Desktop Window Managerの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-70335	GitHub Copilot and Visual Studio Code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-2026-64906	Microsoft Access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-2026-64908	Microsoft Access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-2026-64912	Microsoft Access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-2026-64914	Microsoft Access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-2026-64919	Microsoft Access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-2026-64920	Microsoft Access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-2026-59136	Microsoft COM for Windowsの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-54123	Microsoft Defender for Endpoint for Macの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-62698	Microsoft Digest Authentication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-2026-66301	Microsoft Dynamics 365 (On-Premises)の情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-65815	Microsoft Dynamics 365 On-Premises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-2026-40375	Microsoft Dynamics Business Centralの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-65673	Microsoft Entra Connect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-2026-68797	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-2026-68799	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-2026-68802	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-2026-68808	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-2026-68813	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-2026-70318	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-2026-70327	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-2026-70328	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-2026-65807	Microsoft Excel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-2026-68793	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-2026-68795	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-2026-68796	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-2026-68798	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-2026-68800	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-2026-68801	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-2026-68803	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-2026-68805	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-2026-68806	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-2026-68807	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-2026-68810	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-2026-68811	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-2026-68812	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-2026-68814	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-2026-68815	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-2026-68817	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-2026-62912	Microsoft Exchange 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-2026-62910	Microsoft Exchange Serverの特権昇格の脆弱性	重要	7.2	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65813	Microsoft Exchange Server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-2026-62913	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-2026-62915	Microsoft Exchange Server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-2026-62914	Microsoft Exchange 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-2026-59133	Microsoft High Performance Computing（HPC）Pack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-2026-59124	Microsoft High Performance Computing（HPC）Pack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-2026-62784	Microsoft Local Security Authority Server (lsasrv)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-2026-68792	Microsoft Office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-2026-62842	Microsoft Office 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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-63517	Microsoft Office 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-2026-66809	Microsoft Office 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-2026-63524	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-2026-63529	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-2026-64899	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-2026-70314	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-2026-70315	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-2026-70317	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-2026-70323	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-2026-63533	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-2026-64904	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-2026-65656	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-2026-65661	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-2026-57105	Microsoft Office SharePoint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-2026-70306	Microsoft Office SharePointのなりすましの脆弱性	重要	9.3	いいえ	いいえ	なりすまし
CVE-2026-63521	Microsoft Office 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-2026-63528	Microsoft Office 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-2026-63530	Microsoft Office 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-2026-63531	Microsoft Office 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-2026-64917	Microsoft Office 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-2026-66806	Microsoft Office 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-2026-66810	Microsoft Office 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-2026-70319	Microsoft Office 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-2026-63527	Microsoft Office 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-2026-64905	Microsoft Office 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-2026-64915	Microsoft Office 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-2026-70311	Microsoft Office 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-2026-65680	Microsoft OneDrive for MacOSの特権昇格の脆弱性	重要	6.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-70329	Microsoft Outlook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-2026-62882	Microsoft Outlookのなりすましの脆弱性	重要	4.3	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-2026-70313	Microsoft PowerPoint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-2026-70337	Microsoft PowerShell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-2026-70338	Microsoft PowerShell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-2026-59138	Microsoft Remote Registry Service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-2026-61345	Microsoft Remote Registry Service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-2026-70324	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-2026-70321	Microsoft SharePoint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-2026-70326	Microsoft SharePoint 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-2026-70355	Microsoft SharePoint Server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-2026-62837	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-2026-63514	Microsoft SharePoint 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-2026-63520	Microsoft SharePoint Server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-2026-64901	Microsoft SharePoint 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-2026-65658	Microsoft SharePoint 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-2026-65663	Microsoft SharePoint 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-2026-66805	Microsoft SharePoint 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-2026-66808	Microsoft SharePoint 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-2026-58639	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-2026-62829	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-2026-62839	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-2026-62917	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-2026-63516	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-2026-64897	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-2026-64900	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-2026-64902	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-2026-64916	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-2026-64922	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-2026-65660	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-2026-63512	Microsoft SharePoint Serverの改ざんの脆弱性	重要	6.5	いいえ	いいえ	改ざん
CVE-2026-65767	Microsoft Teams for Android and iOSのなりすましの脆弱性	重要	8.8	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-2026-65769	Microsoft Teams iOSの情報漏洩の脆弱性	重要	6.5	いいえ	いいえ	情報漏洩
CVE-2026-65768	Microsoft Teams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-2026-66804	Microsoft Windows Cross Device 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-2026-59135	Microsoft Windows Search 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-2026-65814	Microsoft Windows Storage Port 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-2026-70310	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-2026-58651	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-2026-6726 ※	MITRE: CVE-2026-6726 TPM 2.0の不適切なオブジェクトスロットの再利用	重要	7.9	いいえ	いいえ	
CVE-2026-6727 ※	MITRE: CVE-2026-6727 TPM 2.0のRSA OAEPタイミングサイドチャネルの脆弱性	重要	5.9	いいえ	いいえ	
CVE-2026-65811	Power BI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-2026-68809	Powerpointの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-70312	Powerpointの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-70316	Powerpointの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-70320	Powerpointの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-70322	Powerpointの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-70325	Powerpointの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-59119	PowerShell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-2026-58612	PowerShellの情報漏洩の脆弱性	重要	7.4	いいえ	いいえ	情報漏洩
CVE-2026-65671	Remote Access 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-2026-65672	Remote Access 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-2026-42976	Remote Access Management service/API (RPC 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-2026-59134	Remote Desktop Client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-2026-61352	Remote Desktop Client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-2026-61363	Remote Desktop Client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-2026-54113	Remote Procedure Call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-2026-62781	RPC Runtime Library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-2026-59125	Virtual Hard Disk (VHD) Miniport 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-2026-47285	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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-54981	Visual Studio Code Python Extension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-2026-59113	Visual Studio Code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-2026-69320	Visual Studio Code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-2026-70336	Visual Studio Code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-2026-58650	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	いいえ	いいえ	セキュリティ機能のバイパス（SFB）
CVE-2026-69278	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	いいえ	いいえ	セキュリティ機能のバイパス（SFB）
CVE-2026-69306	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	いいえ	いいえ	セキュリティ機能のバイパス（SFB）
CVE-2026-62743	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-2026-62746	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-2026-62786	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-2026-62798	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-2026-61358	Windows Accessibility Infrastructure (ATBroker.exe)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-2026-49179	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-2026-61348	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-2026-70307	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-2026-65778	Windows Autopilotの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65779	Windows Autopilotの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65780	Windows Autopilotの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65781	Windows Autopilotの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65782	Windows Autopilotの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65783	Windows Autopilotの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-62908	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-2026-61927	Windows Bind 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-2026-61934	Windows Bind 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-2026-62705	Windows Bind 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-2026-62722	Windows Bind 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-2026-62713	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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-62771	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-2026-62728	Windows Common Log File System 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-2026-62772	Windows Container Isolation FS Filter Driver (unionfs.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-2026-62775	Windows Container Isolation FS Filter Driver (unionfs.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-2026-72971	Windows Container Isolation FS Filter Driver (unionfs.sys)の改ざんの脆弱性	重要	5.5	いいえ	いいえ	改ざん
CVE-2026-61936	Windows Defender Firewall Service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-2026-62710	Windows Device Association 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-2026-62747	Windows Device Association 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-2026-65785	Windows DHCP Client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-2026-62736	Windows DHCP 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-2026-62755	Windows DHCP 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-2026-61361	Windows DHCP Clientのリモートコード実行の脆弱性	重要	7	いいえ	いいえ	リモートコード実行（RCE）
CVE-2026-62761	Windows DHCP 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-2026-62776	Windows DHCP 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-2026-62803	Windows DHCP 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-2026-62807	Windows DHCP 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-2026-62812	Windows DHCP 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-2026-62714	Windows DHCP 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-2026-62715	Windows DHCP 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-2026-62716	Windows DHCP 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-2026-62718	Windows DHCP 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-2026-62720	Windows DHCP 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-2026-62742	Windows DHCP 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-2026-62745	Windows DHCP 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-2026-62814	Windows DHCP 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-2026-61923	Windows Display Enhancement 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-2026-62769	Windows DNSの特権昇格の脆弱性	重要	6.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-62778	Windows DNS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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-62881	Windows DNSの特権昇格の脆弱性	重要	6.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-62883	Windows DNSの特権昇格の脆弱性	重要	6.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65795	Windows DNSの特権昇格の脆弱性	重要	6.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65797	Windows DNSの特権昇格の脆弱性	重要	6.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65798	Windows DNSの特権昇格の脆弱性	重要	6.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-65799	Windows DNSの特権昇格の脆弱性	重要	6.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-70304	Windows DNSの特権昇格の脆弱性	重要	6.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-70330	Windows DNSの特権昇格の脆弱性	重要	6.7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-61920	Windows DNS Serverのリモートコード実行の脆弱性	重要	6.6	いいえ	いいえ	リモートコード実行（RCE）
CVE-2026-62787	Windows DNS 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-2026-61932	Windows 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-2026-62888	Windows 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-2026-62894	Windows 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-2026-61933	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-2026-62703	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-2026-59128	Windows Encrypting File System (EFS)の情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-59126	Windows Event Logging 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-2026-59137	Windows Event Logging 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-2026-61347	Windows Event Logging 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-2026-61360	Windows GDIの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-65662	Windows GDIの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-62709	Windows GDI+の情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-62702	Windows Graphics Kernelのサービス拒否（DoS）の脆弱性	重要	6.8	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-61346	Windows 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-2026-62774	Windows 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-2026-61928	Windows Helloの改ざんの脆弱性	重要	5.5	いいえ	いいえ	改ざん
CVE-2026-62750	Windows HTTP Protocol Stackの改ざんの脆弱性	重要	6.5	いいえ	いいえ	改ざん
CVE-2026-61937	Windows HTTP.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-2026-62735	Windows HTTP.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-2026-62739	Windows HTTP.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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-62741	Windows HTTP.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-2026-62753	Windows HTTP.sysの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-62811	Windows HTTP.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-2026-61368	Windows Hyper-Vの情報漏洩の脆弱性	重要	5	いいえ	いいえ	情報漏洩
CVE-2026-62740	Windows Imaging 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-2026-54984	Windows Imaging 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-2026-59127	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-2026-61925	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-2026-61938	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-2026-62768	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-2026-65774	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-2026-70344	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-2026-70345	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-2026-70346	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-2026-70347	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-2026-65681	Windows iSCSI Target Service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-2026-65796	Windows iSCSI Target Service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-2026-65679	Windows iSCSI Target Service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-2026-62752	Windows Kerberos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-2026-62754	Windows Kerberos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-2026-62766	Windows Kerberosの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-62773	Windows Kerberosの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-61929	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-2026-61930	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-2026-62708	Windows Kernel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-2026-62737	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-2026-62749	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-2026-62780	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-2026-62788	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-2026-65773	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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-62785	Windows LDAP - Lightweight Directory Access Protocol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-2026-62795	Windows LDAP - Lightweight Directory Access Protocol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-2026-62777	Windows License 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-2026-50472	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-2026-62738	Windows Management Instrumentationの情報漏洩の脆弱性	重要	5.5	いいえ	いいえ	情報漏洩
CVE-2026-70348	Windows Management Servicesのサービス拒否（DoS）の脆弱性	重要	5.5	いいえ	いいえ	サービス拒否（DoS）
CVE-2026-62717	Windows Message Queuing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-2026-62719	Windows Message Queuing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-2026-65790	Windows Message Queuing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-2026-62688	Windows MIDI Service Module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-2026-62693	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-2026-62707	Windows Modern Device Management (MDM)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-2026-56174	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-2026-61366	Windows Network Connection Brokerの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-68819	Windows Network File System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-2026-62700	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-2026-62797	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-2026-62880	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-2026-61350	Windows NTFSの情報漏洩の脆弱性	重要	4.6	いいえ	いいえ	情報漏洩
CVE-2026-62793	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-2026-62796	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-2026-62887	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-2026-65784	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-2026-68821	Windows Package Manager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-2026-62696	Windows Program Compatibility Assistant 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-2026-62751	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-2026-62690	Windows Push Notificationsの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-62758	Windows Remote Access Connection 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-2026-62783	Windows Remote Access Connection 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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-61918	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-2026-61921	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-2026-61924	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-2026-61356	Windows Remote Desktop 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-2026-61364	Windows Remote Desktop 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-2026-61365	Windows Remote Desktop 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-2026-61367	Windows Remote Desktop 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-2026-62692	Windows Remote Desktop 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-2026-62779	Windows Schannel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-2026-62757	Windows Schannelのセキュリティ機能のバイパスの脆弱性	重要	5.3	いいえ	いいえ	セキュリティ機能のバイパス（SFB）
CVE-2026-61355	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-2026-62770	Windows Shell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-2026-62799	Windows SMB 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-2026-62782	Windows SMB 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-2026-65794	Windows SMB 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-2026-62790	Windows SMBv3 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-2026-62800	Windows SMBv3 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-2026-61359	Windows Storage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-2026-62695	Windows Storage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-2026-59132	Windows TCP/IP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-2026-62792	Windows TCP/IP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-2026-59122	Windows Telephony 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-2026-61353	Windows Telephony 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-2026-62701	Windows Telephony 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-2026-62723	Windows Telephony 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-2026-62724	Windows Telephony 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-2026-62725	Windows Telephony 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-2026-62726	Windows Telephony 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-2026-62729	Windows Telephony 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-2026-62732	Windows Telephony 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	タイトル	深刻度	CVSS	公開済み	悪用確認	種類
CVE-2026-62734	Windows Telephony 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-2026-62748	Windows Telephony 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-2026-62699	Windows Universal Disk Format File System Driver (UDFS)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-2026-61926	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-2026-62721	Windows User-Mode Power Service (UMPS)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-2026-62711	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-2026-62712	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-2026-62733	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-2026-62876	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-2026-62877	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-2026-62885	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-2026-65678	Windows 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-2026-65775	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-2026-65776	Windows 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-2026-62730	Windows Wired AutoConfig 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-2026-61349	Windows Work Folder 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-2026-61939	Winlogonの特権昇格の脆弱性	重要	7	いいえ	いいえ	特権昇格（EoP）
CVE-2026-56179	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

※が付いたCVE（2件）は、サードパーティが公開し、Microsoftのリリースに含められたものです。
※※が付いたCVE（20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。