Microsoft 2026年11月 セキュリティアップデート

CVE 1,091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）、中（Moderate） | XI：悪用可能性指標

* サードパーティが先に公開し、今回Microsoftのリリースに含められたCVEです。
** Microsoftがすでに修正しており、エンドユーザによる追加対応は不要です。

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-124194	Microsoft Outlook のなりすましの脆弱性	中	6.5	なし	あり	0	なりすまし
CVE-2026-118148	Active Directory Domain Services の特権の昇格の脆弱性	緊急	7.5	なし	なし	1	特権昇格
CVE-2026-114160	Azure Managed Grafana の特権の昇格の脆弱性	緊急	9.8	なし	なし	2	特権昇格
CVE-2026-119990	Azure OpenAI の特権の昇格の脆弱性	緊急	9.8	なし	なし	N/A	特権昇格
CVE-2026-119969	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	2	リモートコード実行
CVE-2026-122194	Microsoft Defender 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	2	リモートコード実行
CVE-2026-118207	Microsoft Exchange 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	1	リモートコード実行
CVE-2026-118292	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-118296	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-118297	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-118701	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-118702	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-118711	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-118713	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-118730	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-120786	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-120788	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-120789	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-124170	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-110043	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	2	リモートコード実行
CVE-2026-110068	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	2	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	XI	種類
CVE-2026-111309	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	2	リモートコード実行
CVE-2026-111289	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	2	リモートコード実行
CVE-2026-120003	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	2	リモートコード実行
CVE-2026-110047	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	2	リモートコード実行
CVE-2026-110067	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	2	リモートコード実行
CVE-2026-111285	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	2	リモートコード実行
CVE-2026-124185	Microsoft Office Word 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	2	リモートコード実行
CVE-2026-120005	Microsoft 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	2	リモートコード実行
CVE-2026-113749	Microsoft Windows Codecs Library 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	2	リモートコード実行
CVE-2026-118737	Remote Procedure Call Runtime 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	2	リモートコード実行
CVE-2026-118146	Windows Active Directory Domain Services 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	1	リモートコード実行
CVE-2026-119962	Windows CredSSP 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	2	リモートコード実行
CVE-2026-119951	Windows Deployment Services 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	2	リモートコード実行
CVE-2026-125134	Windows Function Discovery Resource Publication 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	2	リモートコード実行
CVE-2026-118145	Windows Function Discovery SSDP Provider 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	2	リモートコード実行
CVE-2026-119966	Windows Graphics Kernel の特権の昇格の脆弱性	緊急	7.5	なし	なし	2	特権昇格
CVE-2026-125137	Windows Graphics Kernel の特権の昇格の脆弱性	緊急	7.8	なし	なし	2	特権昇格
CVE-2026-113753	Windows Hyper-V の特権の昇格の脆弱性	緊急	8.2	なし	なし	2	特権昇格
CVE-2026-113856	Windows Hyper-V の特権の昇格の脆弱性	緊急	7.8	なし	なし	2	特権昇格
CVE-2026-113860	Windows Hyper-V の特権の昇格の脆弱性	緊急	7	なし	なし	2	特権昇格
CVE-2026-113861	Windows Hyper-V の特権の昇格の脆弱性	緊急	7.5	なし	なし	2	特権昇格
CVE-2026-113864	Windows Hyper-V の特権の昇格の脆弱性	緊急	6.4	なし	なし	2	特権昇格
CVE-2026-113865	Windows Hyper-V の特権の昇格の脆弱性	緊急	7.8	なし	なし	2	特権昇格
CVE-2026-119947	Windows Hyper-V の特権の昇格の脆弱性	緊急	7.5	なし	なし	2	特権昇格
CVE-2026-119960	Windows Hyper-V の特権の昇格の脆弱性	緊急	7.5	なし	なし	2	特権昇格
CVE-2026-119961	Windows Internet Information Services 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	2	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	XI	種類
CVE-2026-119958	Windows LDAP - Lightweight Directory Access Protocol 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	2	リモートコード実行
CVE-2026-109459	Windows Message Queuing Queue Manager 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	2	リモートコード実行
CVE-2026-119967	Windows Message Queuing Queue Manager 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	2	リモートコード実行
CVE-2026-116710	Windows Message Queuing 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	2	リモートコード実行
CVE-2026-119963	Windows Message Queuing 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	2	リモートコード実行
CVE-2026-119964	Windows Message Queuing 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	2	リモートコード実行
CVE-2026-113862	Windows Network Address Translation (NAT) 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	1	リモートコード実行
CVE-2026-125136	Windows Network Connected Devices Auto-Setup Service 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	2	リモートコード実行
CVE-2026-113752	Windows Print Spooler Components 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	2	リモートコード実行
CVE-2026-114169	Windows 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	2	リモートコード実行
CVE-2026-119957	Windows Remote Desktop Services の特権の昇格の脆弱性	緊急	7.8	なし	なし	2	特権昇格
CVE-2026-113825	Windows SMB Server Network Transport Driver (srvnet.sys) 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	2	リモートコード実行
CVE-2026-119952	Windows Schannel 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	1	リモートコード実行
CVE-2026-116928	Windows Search 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	2	リモートコード実行
CVE-2026-113859	Windows TCP/IP 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	2	リモートコード実行
CVE-2026-119382	Windows TPM の特権の昇格の脆弱性	緊急	7.8	なし	なし	2	特権昇格
CVE-2026-112967	Windows Xbox Live Networking Service 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	2	リモートコード実行
CVE-2026-109475	.NET のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-118747	.NET のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-120796	.NET のサービス拒否の脆弱性	重要	5.3	なし	なし	2	サービス拒否
CVE-2026-105544	.NET の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-114155	.NET の特権の昇格の脆弱性	重要	7.5	なし	なし	N/A	特権昇格
CVE-2026-118746	.NET のセキュリティ機能のバイパスの脆弱性	重要	6.8	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-84004	AMD Zen の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-84005	AMD Zen の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-109478	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-114147	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-114149	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-114154	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-118748	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-118749	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-118750	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-109481	ASP.NET Core の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-114146	ASP.NET Core の特権の昇格の脆弱性	重要	9	なし	なし	2	特権昇格
CVE-2026-118741	ASP.NET Core の特権の昇格の脆弱性	重要	8.1	なし	なし	2	特権昇格
CVE-2026-109476	ASP.NET Core の情報漏洩の脆弱性	重要	6.1	なし	なし	2	情報漏洩
CVE-2026-114150	ASP.NET Core の情報漏洩の脆弱性	重要	5.9	なし	なし	2	情報漏洩
CVE-2026-114156	ASP.NET Core 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	2	セキュリティ機能のバイパス
CVE-2026-114157	ASP.NET Core 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	2	セキュリティ機能のバイパス
CVE-2026-118735	Active Directory Domain Services の特権の昇格の脆弱性	重要	7.5	なし	なし	3	特権昇格
CVE-2026-123387	Active Directory Domain Services の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-119889	ActiveSyncProvider の情報漏洩の脆弱性	重要	6.5	なし	なし	3	情報漏洩
CVE-2026-120006	Aspire の特権の昇格の脆弱性	重要		なし	なし	2	特権昇格
CVE-2026-120778	Aspire の特権の昇格の脆弱性	重要	7.3	なし	なし	2	特権昇格
CVE-2026-120792	Aspire の情報漏洩の脆弱性	重要	7.3	なし	なし	2	情報漏洩
CVE-2026-118740	Aspire のセキュリティ機能のバイパスの脆弱性	重要	9.1	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-109457	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	2	リモートコード実行
CVE-2026-121668	Azure Confidential Clean Rooms の改ざんの脆弱性	重要		なし	なし	2	改ざん
CVE-2026-102224	Azure CycleCloud の特権の昇格の脆弱性	重要	8.4	なし	なし	2	特権昇格
CVE-2026-113822	Azure CycleCloud の特権の昇格の脆弱性	重要	6.5	なし	なし	N/A	特権昇格
CVE-2026-114161	Azure CycleCloud の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-113823	Azure CycleCloud の情報漏洩の脆弱性	重要	7.5	なし	なし	2	情報漏洩
CVE-2026-120783	Azure DevOps Server の特権の昇格の脆弱性	重要	6.4	なし	なし	2	特権昇格
CVE-2026-85923	Azure DevOps Server の特権の昇格の脆弱性	重要	8.8	なし	なし	N/A	特権昇格
CVE-2026-112745	Azure DevOps Server の情報漏洩の脆弱性	重要	6.5	なし	なし	1	情報漏洩
CVE-2026-109467	Azure DevOps Server のリモートでコードが実行される脆弱性	重要	9.9	なし	なし	N/A	リモートコード実行
CVE-2026-109462	Azure Firmware 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	2	セキュリティ機能のバイパス
CVE-2026-118742	Azure Front Door の特権の昇格の脆弱性	重要	8.6	なし	なし	N/A	特権昇格
CVE-2026-105494	Azure NFS mount helper (aznfs) の特権の昇格の脆弱性	重要		なし	なし	2	特権昇格
CVE-2026-119989	Azure Pipelines のリモートでコードが実行される脆弱性	重要	8.2	なし	なし	2	リモートコード実行
CVE-2026-96007	Connected Devices Platform Service (Cdpsvc) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119883	Data Deduplication のセキュリティ機能のバイパスの脆弱性	重要	3.3	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-95963	Data Sharing Service Client の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-105528	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105581	Desktop Window Manager の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-113819	Desktop Window Manager の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格
CVE-2026-96103	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96172	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96174	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96175	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-94507	DirectX の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-83953	GitHub Copilot for Jetbrains の情報漏洩の脆弱性	重要	5.5	なし	なし	N/A	情報漏洩
CVE-2026-96084	Graphic Fonts の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-88211	Graphic Fonts の情報漏洩の脆弱性	重要	5.7	なし	なし	2	情報漏洩
CVE-2026-100204	HEIF Image Extensions 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	2	リモートコード実行
CVE-2026-114164	HEVC Video Extensions 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	2	リモートコード実行
CVE-2026-114165	HEVC Video 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	2	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	XI	種類
CVE-2026-114167	HEVC Video 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	2	リモートコード実行
CVE-2026-122173	HID Parser Library の特権の昇格の脆弱性	重要	6.8	なし	なし	2	特権昇格
CVE-2026-125135	HID Parser Library の特権の昇格の脆弱性	重要	6.8	なし	なし	2	特権昇格
CVE-2026-96010	HID Parser Library の特権の昇格の脆弱性	重要	8.8	なし	なし	3	特権昇格
CVE-2026-96974	HID Parser Library の特権の昇格の脆弱性	重要	6.8	なし	なし	3	特権昇格
CVE-2026-96979	HID Parser Library の特権の昇格の脆弱性	重要	6.8	なし	なし	3	特権昇格
CVE-2026-96982	HID Parser Library の特権の昇格の脆弱性	重要	6.8	なし	なし	3	特権昇格
CVE-2026-96059	HID class driver の情報漏洩の脆弱性	重要	5.5	なし	なし	3	情報漏洩
CVE-2026-119942	HTTP.sys の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-119946	HTTP.sys の情報漏洩の脆弱性	重要	5.9	なし	なし	2	情報漏洩
CVE-2026-70003	JDBC Driver for SQL Server のセキュリティ機能のバイパスの脆弱性	重要	8.7	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-119937	Kernel Streaming Service Driver の特権の昇格の脆弱性	重要	6.6	なし	なし	2	特権昇格
CVE-2026-105537	Mailslot File System の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-109485	Microsoft 365 Agents SDK の情報漏洩の脆弱性	重要	6.3	なし	なし	2	情報漏洩
CVE-2026-112974	Microsoft Account の改ざんの脆弱性	重要	5.5	なし	なし	2	改ざん
CVE-2026-112982	Microsoft Account の改ざんの脆弱性	重要	5.5	なし	なし	2	改ざん
CVE-2026-96158	Microsoft ActiveX Installer Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-108470	Microsoft Authentication Library (MSAL) for Node.js の情報漏洩の脆弱性	重要		なし	なし	2	情報漏洩
CVE-2026-108469	Microsoft Authentication Library for JavaScript のなりすましの脆弱性	重要	6.8	なし	なし	2	なりすまし
CVE-2026-118288	Microsoft Azure File Sync の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-70120	Microsoft Bluetooth Driver の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-85929	Microsoft Brokering File System の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96054	Microsoft Color Management 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	2	リモートコード実行
CVE-2026-96067	Microsoft Color Management 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	2	リモートコード実行
CVE-2026-96078	Microsoft Color Management 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	2	リモートコード実行
CVE-2026-119991	Microsoft Configuration Manager の情報漏洩の脆弱性	重要	5.9	なし	なし	2	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-95882	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	2	リモートコード実行
CVE-2026-95891	Microsoft DirectMusic 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	2	リモートコード実行
CVE-2026-95896	Microsoft DirectMusic 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	2	リモートコード実行
CVE-2026-95901	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	2	リモートコード実行
CVE-2026-122196	Microsoft Dynamics 365 (on-premises) の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-109460	Microsoft Entra Private Network Connector の情報漏洩の脆弱性	重要	5.5	なし	なし	N/A	情報漏洩
CVE-2026-118153	Microsoft Exchange Server のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-118150	Microsoft Exchange Server の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118151	Microsoft Exchange Server の特権の昇格の脆弱性	重要	7.2	なし	なし	2	特権昇格
CVE-2026-118154	Microsoft Exchange Server の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118157	Microsoft Exchange Server の特権の昇格の脆弱性	重要	7.2	なし	なし	2	特権昇格
CVE-2026-118149	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	3	リモートコード実行
CVE-2026-118152	Microsoft Exchange Server のなりすましの脆弱性	重要	6.5	なし	なし	2	なりすまし
CVE-2026-118208	Microsoft Exchange Server のなりすましの脆弱性	重要	7.1	なし	なし	2	なりすまし
CVE-2026-114162	Microsoft Graph の特権の昇格の脆弱性	重要	9.1	なし	なし	2	特権昇格
CVE-2026-112754	Microsoft Graphics Component の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-122987	Microsoft High Performance Computing (HPC) Pack の特権の昇格の脆弱性	重要	5.9	なし	なし	2	特権昇格
CVE-2026-105505	Microsoft Input Method Editor (IME) の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105578	Microsoft JScript 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	2	リモートコード実行
CVE-2026-109492	Microsoft MCP Gateway の特権の昇格の脆弱性	重要		なし	なし	N/A	特権昇格
CVE-2026-108411	Microsoft ODBC 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	2	リモートコード実行
CVE-2026-109493	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	2	リモートコード実行
CVE-2026-109498	Microsoft Office Access 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	2	リモートコード実行
CVE-2026-110058	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	2	リモートコード実行
CVE-2026-110059	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	2	リモートコード実行
CVE-2026-110060	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	2	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	XI	種類
CVE-2026-111301	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	2	リモートコード実行
CVE-2026-111305	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	2	リモートコード実行
CVE-2026-118715	Microsoft Office Excel の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118725	Microsoft Office Excel の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-111292	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-118300	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-118727	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-118728	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-119999	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-123395	Microsoft Office Excel の情報漏洩の脆弱性	重要	5.9	なし	なし	2	情報漏洩
CVE-2026-124178	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-124179	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-124183	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-116927	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	2	リモートコード実行
CVE-2026-118293	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	2	リモートコード実行
CVE-2026-118294	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	2	リモートコード実行
CVE-2026-118295	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	2	リモートコード実行
CVE-2026-118298	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	2	リモートコード実行
CVE-2026-118299	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	2	リモートコード実行
CVE-2026-118301	Microsoft Office Excel 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	2	リモートコード実行
CVE-2026-118302	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	2	リモートコード実行
CVE-2026-118700	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	2	リモートコード実行
CVE-2026-118703	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	2	リモートコード実行
CVE-2026-118704	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	2	リモートコード実行
CVE-2026-118705	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	2	リモートコード実行
CVE-2026-118706	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	2	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	XI	種類
CVE-2026-118707	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	2	リモートコード実行
CVE-2026-118708	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	2	リモートコード実行
CVE-2026-118709	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	2	リモートコード実行
CVE-2026-118710	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	2	リモートコード実行
CVE-2026-118712	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	2	リモートコード実行
CVE-2026-118714	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	2	リモートコード実行
CVE-2026-118716	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	2	リモートコード実行
CVE-2026-118717	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	2	リモートコード実行
CVE-2026-118718	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	2	リモートコード実行
CVE-2026-118719	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	2	リモートコード実行
CVE-2026-118720	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	2	リモートコード実行
CVE-2026-118721	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	2	リモートコード実行
CVE-2026-118722	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	2	リモートコード実行
CVE-2026-118723	Microsoft Office 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	2	リモートコード実行
CVE-2026-118724	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	2	リモートコード実行
CVE-2026-118726	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	2	リモートコード実行
CVE-2026-118729	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	2	リモートコード実行
CVE-2026-118731	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	2	リモートコード実行
CVE-2026-118732	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	2	リモートコード実行
CVE-2026-119986	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	2	リモートコード実行
CVE-2026-120785	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	3	リモートコード実行
CVE-2026-120790	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	2	リモートコード実行
CVE-2026-120791	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	2	リモートコード実行
CVE-2026-123385	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	2	リモートコード実行
CVE-2026-124174	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	2	リモートコード実行
CVE-2026-124176	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	2	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	XI	種類
CVE-2026-124187	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	2	リモートコード実行
CVE-2026-124229	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	6.6	なし	なし	2	リモートコード実行
CVE-2026-111291	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-111293	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-112731	Microsoft Office の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-119993	Microsoft Office Outlook の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-119995	Microsoft Office Outlook 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	2	リモートコード実行
CVE-2026-119996	Microsoft Office Outlook 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	2	リモートコード実行
CVE-2026-119997	Microsoft Office Outlook 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	2	リモートコード実行
CVE-2026-123375	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	2	リモートコード実行
CVE-2026-123376	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	2	リモートコード実行
CVE-2026-123377	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	2	リモートコード実行
CVE-2026-123378	Microsoft Office Outlook 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	2	リモートコード実行
CVE-2026-123379	Microsoft Office Outlook 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	2	リモートコード実行
CVE-2026-123380	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	2	リモートコード実行
CVE-2026-123381	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	2	リモートコード実行
CVE-2026-123382	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	2	リモートコード実行
CVE-2026-123383	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	2	リモートコード実行
CVE-2026-123384	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	2	リモートコード実行
CVE-2026-124227	Microsoft Office Outlook 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	2	リモートコード実行
CVE-2026-124228	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	2	リモートコード実行
CVE-2026-112738	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-116922	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-112734	Microsoft Office PowerPoint 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	2	リモートコード実行
CVE-2026-112737	Microsoft Office PowerPoint 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	2	リモートコード実行
CVE-2026-120001	Microsoft Office PowerPoint 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	2	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	XI	種類
CVE-2026-111286	Microsoft Office 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	2	リモートコード実行
CVE-2026-116717	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	2	リモートコード実行
CVE-2026-122198	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	2	リモートコード実行
CVE-2026-119998	Microsoft Office 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	2	セキュリティ機能のバイパス
CVE-2026-109466	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-109495	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	6.6	なし	なし	2	特権昇格
CVE-2026-109502	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-111296	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-123391	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	3	特権昇格
CVE-2026-80095	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	9	なし	なし	2	特権昇格
CVE-2026-88176	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-109455	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-110057	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-124210	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-109464	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	2	リモートコード実行
CVE-2026-109472	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	2	リモートコード実行
CVE-2026-109499	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	2	リモートコード実行
CVE-2026-110044	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	2	リモートコード実行
CVE-2026-120000	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	2	リモートコード実行
CVE-2026-123390	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	N/A	リモートコード実行
CVE-2026-109454	Microsoft Office SharePoint のなりすましの脆弱性	重要	9	なし	なし	2	なりすまし
CVE-2026-109456	Microsoft Office SharePoint のなりすましの脆弱性	重要	4.6	なし	なし	2	なりすまし
CVE-2026-109497	Microsoft Office SharePoint のなりすましの脆弱性	重要	7.3	なし	なし	2	なりすまし
CVE-2026-109504	Microsoft Office SharePoint のなりすましの脆弱性	重要	7.3	なし	なし	2	なりすまし
CVE-2026-110045	Microsoft Office SharePoint のなりすましの脆弱性	重要	7.3	なし	なし	2	なりすまし
CVE-2026-110065	Microsoft Office SharePoint のなりすましの脆弱性	重要	7.3	なし	なし	2	なりすまし

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-111297	Microsoft Office SharePoint のなりすましの脆弱性	重要	8	なし	なし	2	なりすまし
CVE-2026-111300	Microsoft Office SharePoint のなりすましの脆弱性	重要	7.3	なし	なし	2	なりすまし
CVE-2026-111303	Microsoft Office SharePoint のなりすましの脆弱性	重要	7.3	なし	なし	2	なりすまし
CVE-2026-112736	Microsoft Office SharePoint のなりすましの脆弱性	重要	5.3	なし	なし	2	なりすまし
CVE-2026-109494	Microsoft Office Visio 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	2	リモートコード実行
CVE-2026-109496	Microsoft Office Visio 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	2	リモートコード実行
CVE-2026-110046	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-110051	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-110066	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-111288	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-112720	Microsoft Office Word の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-116721	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-124233	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-109491	Microsoft Office Word 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	2	リモートコード実行
CVE-2026-109500	Microsoft Office Word 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	2	リモートコード実行
CVE-2026-109501	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	2	リモートコード実行
CVE-2026-109503	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	2	リモートコード実行
CVE-2026-109505	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	2	リモートコード実行
CVE-2026-110050	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	2	リモートコード実行
CVE-2026-110052	Microsoft Office Word 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	2	リモートコード実行
CVE-2026-110053	Microsoft Office Word 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	2	リモートコード実行
CVE-2026-110054	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	2	リモートコード実行
CVE-2026-110056	Microsoft Office 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	2	リモートコード実行
CVE-2026-110061	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	2	リモートコード実行
CVE-2026-110062	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	2	リモートコード実行
CVE-2026-110064	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	2	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	XI	種類
CVE-2026-111287	Microsoft Office Word 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	2	リモートコード実行
CVE-2026-111290	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	2	リモートコード実行
CVE-2026-111294	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	2	リモートコード実行
CVE-2026-111295	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	2	リモートコード実行
CVE-2026-111298	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	2	リモートコード実行
CVE-2026-111299	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	2	リモートコード実行
CVE-2026-111302	Microsoft Office 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	2	リモートコード実行
CVE-2026-111304	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	2	リモートコード実行
CVE-2026-111306	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	2	リモートコード実行
CVE-2026-111307	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	2	リモートコード実行
CVE-2026-111308	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	2	リモートコード実行
CVE-2026-111310	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	2	リモートコード実行
CVE-2026-112714	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	2	リモートコード実行
CVE-2026-112715	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	2	リモートコード実行
CVE-2026-112716	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	2	リモートコード実行
CVE-2026-112717	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	2	リモートコード実行
CVE-2026-112718	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	2	リモートコード実行
CVE-2026-112719	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	2	リモートコード実行
CVE-2026-112721	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	2	リモートコード実行
CVE-2026-112722	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	2	リモートコード実行
CVE-2026-112723	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	2	リモートコード実行
CVE-2026-112724	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	2	リモートコード実行
CVE-2026-112726	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	2	リモートコード実行
CVE-2026-112728	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	2	リモートコード実行
CVE-2026-112729	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	2	リモートコード実行
CVE-2026-112730	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	2	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	XI	種類
CVE-2026-112733	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	2	リモートコード実行
CVE-2026-112735	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	2	リモートコード実行
CVE-2026-112739	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	2	リモートコード実行
CVE-2026-112741	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	2	リモートコード実行
CVE-2026-116718	Microsoft Office Word 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	2	リモートコード実行
CVE-2026-116719	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	2	リモートコード実行
CVE-2026-116720	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	2	リモートコード実行
CVE-2026-116722	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	2	リモートコード実行
CVE-2026-116923	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	2	リモートコード実行
CVE-2026-116925	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	2	リモートコード実行
CVE-2026-123394	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	2	リモートコード実行
CVE-2026-109487	Microsoft PowerPoint 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	2	リモートコード実行
CVE-2026-122985	Microsoft PowerShell の情報漏洩の脆弱性	重要	6.1	なし	なし	2	情報漏洩
CVE-2026-113815	Microsoft PowerShell 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	2	セキュリティ機能のバイパス
CVE-2026-124226	Microsoft PowerShell 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	2	セキュリティ機能のバイパス
CVE-2026-105512	Microsoft QUIC のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-88236	Microsoft QUIC のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-114166	Microsoft Raw Image Extension の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-105492	Microsoft Remote Registry Service のサービス拒否の脆弱性	重要	5.3	なし	なし	2	サービス拒否
CVE-2026-116929	Microsoft SQL Server の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-116934	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-116944	Microsoft SQL Server の特権の昇格の脆弱性	重要	7.2	なし	なし	2	特権昇格
CVE-2026-118105	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118108	Microsoft SQL Server の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-118109	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118110	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-118111	Microsoft SQL Server の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-118112	Microsoft SQL Server の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-118113	Microsoft SQL Server の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-118114	Microsoft SQL Server の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-118115	Microsoft SQL Server の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-118116	Microsoft SQL Server の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-118117	Microsoft SQL Server の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-118118	Microsoft SQL Server の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-118119	Microsoft SQL Server の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-118120	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-66813	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.1	なし	なし	2	特権昇格
CVE-2026-67375	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-67387	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-84010	Microsoft SQL Server の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-94513	Microsoft SQL Server の特権の昇格の脆弱性	重要	8	なし	なし	3	特権昇格
CVE-2026-116932	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-116935	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-116939	Microsoft SQL Server の情報漏洩の脆弱性	重要	5.7	なし	なし	2	情報漏洩
CVE-2026-116940	Microsoft SQL Server の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-116943	Microsoft SQL Server の情報漏洩の脆弱性	重要	7.5	なし	なし	2	情報漏洩
CVE-2026-118102	Microsoft SQL Server の情報漏洩の脆弱性	重要	5.9	なし	なし	2	情報漏洩
CVE-2026-118103	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-118104	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-67382	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-68783	Microsoft SQL Server の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-116930	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	2	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	XI	種類
CVE-2026-116931	Microsoft SQL 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	2	リモートコード実行
CVE-2026-116933	Microsoft SQL Server のリモートでコードが実行される脆弱性	重要	7.2	なし	なし	2	リモートコード実行
CVE-2026-116936	Microsoft SQL Server のリモートでコードが実行される脆弱性	重要	7.2	なし	なし	2	リモートコード実行
CVE-2026-116937	Microsoft SQL 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	2	リモートコード実行
CVE-2026-116938	Microsoft SQL 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	2	リモートコード実行
CVE-2026-116941	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	2	リモートコード実行
CVE-2026-116942	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	2	リモートコード実行
CVE-2026-116945	Microsoft SQL Server 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	2	リモートコード実行
CVE-2026-116946	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	2	リモートコード実行
CVE-2026-116947	Microsoft SQL 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	2	リモートコード実行
CVE-2026-118106	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	2	リモートコード実行
CVE-2026-67372	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	2	リモートコード実行
CVE-2026-67374	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	2	リモートコード実行
CVE-2026-67391	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	3	リモートコード実行
CVE-2026-67632	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	3	リモートコード実行
CVE-2026-67637	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	3	リモートコード実行
CVE-2026-67646	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	3	リモートコード実行
CVE-2026-120002	Microsoft SharePoint Server の特権の昇格の脆弱性	重要	9.9	なし	なし	2	特権昇格
CVE-2026-116926	Microsoft Teams のなりすましの脆弱性	重要	7.5	なし	なし	2	なりすまし
CVE-2026-122979	Microsoft Teams for Android のなりすましの脆弱性	重要	8.1	なし	なし	N/A	なりすまし
CVE-2026-69901	Microsoft Teams for Android のなりすましの脆弱性	重要	7.5	なし	なし	N/A	なりすまし
CVE-2026-121681	Microsoft Trace Data Helper の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-122172	Microsoft Trace Data Helper の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-116698	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	7.5	なし	なし	2	リモートコード実行
CVE-2026-116699	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	6.5	なし	なし	3	リモートコード実行
CVE-2026-85838	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	2	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	XI	種類
CVE-2026-85839	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	2	リモートコード実行
CVE-2026-88222	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	2	リモートコード実行
CVE-2026-119987	Microsoft Windows App Store の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96150	Microsoft Windows Codecs Library の情報漏洩の脆弱性	重要	5.6	なし	なし	2	情報漏洩
CVE-2026-122168	Microsoft Windows Media Foundation の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96157	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	2	リモートコード実行
CVE-2026-105586	Microsoft Windows SCSI Class System File の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-113821	Microsoft Windows SCSI Class System File の情報漏洩の脆弱性	重要	4.1	なし	なし	3	情報漏洩
CVE-2026-119943	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119954	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119904	Microsoft Windows Speech の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-97002	Microsoft Windows VMSwitch の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-110048	Microsoft 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	2	リモートコード実行
CVE-2026-110049	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	2	リモートコード実行
CVE-2026-110055	Microsoft 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	2	リモートコード実行
CVE-2026-113759	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	2	リモートコード実行
CVE-2026-119881	Microsoft XPS Document Converter の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-119880	Microsoft XPS Document Converter 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	2	リモートコード実行
CVE-2026-122171	Microsoft XPS Document Converter 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	2	リモートコード実行
CVE-2026-66801	Microsoft Xbox のリモートでコードが実行される脆弱性	重要		なし	なし	2	リモートコード実行
CVE-2026-62903	Microsoft.Data.SqlClient の情報漏洩の脆弱性	重要		なし	なし	2	情報漏洩
CVE-2026-124224	PowerShell の特権の昇格の脆弱性	重要	7	なし	なし	3	特権昇格
CVE-2026-121669	PowerShell の情報漏洩の脆弱性	重要	6.1	なし	なし	2	情報漏洩
CVE-2026-121674	PowerShell の情報漏洩の脆弱性	重要	6.1	なし	なし	2	情報漏洩
CVE-2026-121675	PowerShell の情報漏洩の脆弱性	重要	6.1	なし	なし	2	情報漏洩
CVE-2026-119387	Quality Windows Audio/Video Experience (QWAVE) service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-119388	Quality Windows Audio/Video Experience (QWAVE) service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-123389	Quality Windows Audio/Video Experience (QWAVE) service の特権の昇格の脆弱性	重要	7	なし	なし	3	特権昇格
CVE-2026-83894	RPC Runtime の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-116697	Reliable Multicast Transport Driver (RMCAST) のサービス拒否の脆弱性	重要	5.9	なし	なし	2	サービス拒否
CVE-2026-119853	Remote Access API の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-119390	Remote Desktop Client 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	2	リモートコード実行
CVE-2026-119858	Remote Desktop Client 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	2	リモートコード実行
CVE-2026-119934	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	2	リモートコード実行
CVE-2026-95964	Remote Desktop Client 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	3	リモートコード実行
CVE-2026-119824	Remote Desktop Client の改ざんの脆弱性	重要	8.8	なし	なし	2	改ざん
CVE-2026-80094	Remote Desktop Gateway Service の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-108401	Remote Desktop Services 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	2	リモートコード実行
CVE-2026-119972	Remote Procedure Call のサービス拒否の脆弱性	重要	5.9	なし	なし	2	サービス拒否
CVE-2026-96017	Role: DNS Server のサービス拒否の脆弱性	重要	4.9	なし	なし	3	サービス拒否
CVE-2026-96975	Role: DNS Server のサービス拒否の脆弱性	重要	5.9	なし	なし	2	サービス拒否
CVE-2026-88111	SQL 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	2	リモートコード実行
CVE-2026-94511	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	3	リモートコード実行
CVE-2026-96989	Secondary Logon の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-118140	Server for NFS の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-88235	Servicing Stack Updates の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-113748	Software Protection Platform (SPP) の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119395	Storport.sys Driver の情報漏洩の脆弱性	重要	4	なし	なし	2	情報漏洩
CVE-2026-119849	Virtual Hard Disk (VHD) Miniport Driver 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	2	リモートコード実行
CVE-2026-119981	Visual Studio Code の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119976	Visual Studio Code GitHub Pull Requests and Issues Extension の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-102230	Visual Studio Code の情報漏洩の脆弱性	重要	7.4	なし	なし	2	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-119975	Visual Studio Code 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	2	リモートコード実行
CVE-2026-119985	Visual Studio Code のリモートでコードが実行される脆弱性	重要	8.3	なし	なし	2	リモートコード実行
CVE-2026-120779	Visual Studio Code のリモートでコードが実行される脆弱性	重要	9.6	なし	なし	2	リモートコード実行
CVE-2026-120780	Visual Studio Code のリモートでコードが実行される脆弱性	重要	8.3	なし	なし	2	リモートコード実行
CVE-2026-121662	Visual Studio Code のリモートでコードが実行される脆弱性	重要	8.6	なし	なし	1	リモートコード実行
CVE-2026-121664	Visual Studio Code のリモートでコードが実行される脆弱性	重要	8.3	なし	なし	2	リモートコード実行
CVE-2026-70094	Visual Studio Code 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	2	リモートコード実行
CVE-2026-102236	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	8.6	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-114171	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	2	セキュリティ機能のバイパス
CVE-2026-119982	Visual Studio Code 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	2	セキュリティ機能のバイパス
CVE-2026-119983	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	2	セキュリティ機能のバイパス
CVE-2026-120782	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	2	セキュリティ機能のバイパス
CVE-2026-121660	Visual Studio Code 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	2	セキュリティ機能のバイパス
CVE-2026-121661	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	2	セキュリティ機能のバイパス
CVE-2026-121663	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	1	セキュリティ機能のバイパス
CVE-2026-121665	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	2	セキュリティ機能のバイパス
CVE-2026-114151	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	2	リモートコード実行
CVE-2026-114152	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	2	リモートコード実行
CVE-2026-114158	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	2	リモートコード実行
CVE-2026-114159	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	2	リモートコード実行
CVE-2026-118745	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	2	リモートコード実行
CVE-2026-105017	Volume Shadow Copy の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119941	Volume Shadow Copy の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119825	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-119856	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-119910	Win32k の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-95893	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-112727	Windows Domain Name 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	2	リモートコード実行
CVE-2026-96002	Windows Domain Name 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	2	リモートコード実行
CVE-2026-96020	Windows Domain Name 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	2	リモートコード実行
CVE-2026-96064	Windows Domain Name 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	2	リモートコード実行
CVE-2026-96092	Windows Domain Name Service 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	3	リモートコード実行
CVE-2026-96177	Windows Domain Name Service 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	2	リモートコード実行
CVE-2026-95884	Windows Active Directory Certificate Services の情報漏洩の脆弱性	重要	5.3	なし	なし	2	情報漏洩
CVE-2026-105590	Windows Active Directory Certificate Services のセキュリティ機能のバイパスの脆弱性	重要	5.3	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-105559	Windows Active Directory のサービス拒否の脆弱性	重要	6.5	なし	なし	2	サービス拒否
CVE-2026-105568	Windows Active Directory Domain Services のサービス拒否の脆弱性	重要	6.5	なし	なし	2	サービス拒否
CVE-2026-119948	Windows Active Directory 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	2	リモートコード実行
CVE-2026-122988	Windows Admin Center の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-105020	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105021	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105022	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105023	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105025	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105026	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105490	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105491	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105493	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105495	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105496	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105497	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105498	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-105499	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118215	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-118216	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118217	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118218	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118219	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118221	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118222	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-118223	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-118224	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-118225	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118226	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118227	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118228	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118229	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118232	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118277	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118278	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118279	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118280	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-118283	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-94515	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95960	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-118214	Windows Advanced Rasterization Platform の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-88242	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格
CVE-2026-95944	Windows App Readiness Service の改ざんの脆弱性	重要	5.5	なし	なし	2	改ざん

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-96018	Windows AppContainer の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-116714	Windows AppX Deployment Service の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-88224	Windows AppX Deployment Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96074	Windows AppX Package Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105541	Windows Audio Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119888	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119893	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119894	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119895	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-121671	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96038	Windows Audio Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96155	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-122175	Windows Autopilot の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格
CVE-2026-105554	Windows Background Intelligent Transfer Service (BITS) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119405	Windows Backup Engine の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-70182	Windows Bind Filter Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	3	特権昇格
CVE-2026-88239	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95877	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96127	Windows Biometric Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119832	Windows BitLocker のセキュリティ機能のバイパスの脆弱性	重要	5.9	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-97015	Windows BitLocker のセキュリティ機能のバイパスの脆弱性	重要	6.8	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-88187	Windows Bluetooth A2DP driver の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-95996	Windows Bluetooth Port Driver の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-88213	Windows Bluetooth Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96001	Windows Bluetooth Service の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-112761	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-113762	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119401	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119402	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119403	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-88221	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-94529	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95871	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96156	Windows Broker Infrastructure Service の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-88245	Windows Brokering File System の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95979	Windows Brokering File System の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96097	Windows Brokering File System の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-108405	Windows CD-ROM Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-108404	Windows CD-ROM Driver 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	2	リモートコード実行
CVE-2026-103571	Windows CNG Key Isolation Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105533	Windows COM の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112968	Windows COM の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-94531	Windows COM の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-113767	Windows COM+ Event System Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-113769	Windows COM+ Event System Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119855	Windows COM+ Event System Service の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-85942	Windows Camera Frame Server Monitor の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-88232	Windows Camera Frame Server Monitor の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-88238	Windows Camera Frame Server Monitor の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-118138	Windows Client for NFS の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-122165	Windows Client for NFS の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95885	Windows Client for NFS の特権の昇格の脆弱性	重要	8.1	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-118141	Windows Client for NFS 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	3	リモートコード実行
CVE-2026-88249	Windows Client for NFS 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	2	リモートコード実行
CVE-2026-119404	Windows Client for NFS のセキュリティ機能のバイパスの脆弱性	重要	5.9	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-96162	Windows Clipboard Virtual Channel Extension の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105569	Windows Cloud Files Mini Filter Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112763	Windows Cloud Files Mini Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	3	特権昇格
CVE-2026-112810	Windows Cloud Files Mini Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119974	Windows Cloud Files Mini Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112803	Windows Cloud Files Mini Filter Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-112809	Windows Composite Image File System の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-96072	Windows Connected User Experiences and Telemetry の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96088	Windows Connected User Experiences and Telemetry の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96101	Windows Connected User Experiences and Telemetry の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-96042	Windows Connection Manager Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96043	Windows Connection Manager Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112753	Windows Container Isolation FS Filter Driver (unionfs.sys) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-113761	Windows Container Isolation FS Filter Driver (unionfs.sys) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-113771	Windows Container Isolation FS Filter Driver (unionfs.sys) の特権の昇格の脆弱性	重要	5.5	なし	なし	2	特権昇格
CVE-2026-105562	Windows Container Manager Service の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-119393	Windows Credential Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	3	特権昇格
CVE-2026-96978	Windows Credential User Interface の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-118739	Windows DHCP Client のサービス拒否の脆弱性	重要	6.5	なし	なし	2	サービス拒否
CVE-2026-113863	Windows DHCP Client の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-88240	Windows DHCP Client の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-96115	Windows DHCP Client の特権の昇格の脆弱性	重要	8	なし	なし	2	特権昇格
CVE-2026-119890	Windows DHCP Server のサービス拒否の脆弱性	重要	5.3	なし	なし	2	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-96134	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-105588	Windows DHCP Server の特権の昇格の脆弱性	重要	6.4	なし	なし	2	特権昇格
CVE-2026-105557	Windows DHCP Server の情報漏洩の脆弱性	重要	5.9	なし	なし	2	情報漏洩
CVE-2026-105560	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	7.2	なし	なし	2	リモートコード実行
CVE-2026-72998	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	2	リモートコード実行
CVE-2026-88216	Windows DHCP 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	2	リモートコード実行
CVE-2026-88243	Windows DHCP Server 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	2	リモートコード実行
CVE-2026-113773	Windows DHCP Server のなりすましの脆弱性	重要	5.3	なし	なし	2	なりすまし
CVE-2026-96076	Windows DIAL Client の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96176	Windows DNS のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-96983	Windows DNS のサービス拒否の脆弱性	重要	5.3	なし	なし	3	サービス拒否
CVE-2026-105520	Windows DNS の特権の昇格の脆弱性	重要	7.2	なし	なし	2	特権昇格
CVE-2026-119953	Windows DNS の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96179	Windows DNS の特権の昇格の脆弱性	重要	6.7	なし	なし	2	特権昇格
CVE-2026-105579	Windows DNS の情報漏洩の脆弱性	重要	7.5	なし	なし	2	情報漏洩
CVE-2026-108425	Windows DNS の情報漏洩の脆弱性	重要	5.9	なし	なし	2	情報漏洩
CVE-2026-119970	Windows DNS の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-96970	Windows DNS の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-96976	Windows DNS の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-96980	Windows DNS の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-96984	Windows DNS の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-96985	Windows DNS の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-96986	Windows DNS の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-96987	Windows DNS の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-96988	Windows DNS の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-97006	Windows DNS の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-109463	Windows DNS 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	2	リモートコード実行
CVE-2026-113855	Windows DNS 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	2	リモートコード実行
CVE-2026-88218	Windows DNS 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	2	リモートコード実行
CVE-2026-119971	Windows DNS Server の情報漏洩の脆弱性	重要	4.9	なし	なし	2	情報漏洩
CVE-2026-96112	Windows DNS Server の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-96972	Windows DNS Server の情報漏洩の脆弱性	重要	7.5	なし	なし	2	情報漏洩
CVE-2026-81384	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	2	リモートコード実行
CVE-2026-119905	Windows DNS のなりすましの脆弱性	重要	4.9	なし	なし	2	なりすまし
CVE-2026-113763	Windows DPAPI (Data Protection Application Programming Interface) の特権の昇格の脆弱性	重要	6.3	なし	なし	3	特権昇格
CVE-2026-105575	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105582	Windows DWM Core Library の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105583	Windows DWM Core Library の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112986	Windows DWM Core Library の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112758	Windows Defender Firewall Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112977	Windows Deployment Services の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-113818	Windows Deployment Services の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-118213	Windows Deployment Services の情報漏洩の脆弱性	重要	5.9	なし	なし	2	情報漏洩
CVE-2026-105558	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	2	リモートコード実行
CVE-2026-112988	Windows Desktop Window Manager の特権の昇格の脆弱性	重要	5.5	なし	なし	2	特権昇格
CVE-2026-113758	Windows Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112743	Windows Device Association Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119844	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119866	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119874	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-113750	Windows Device Inventory の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-113817	Windows Devices Human Interface の特権の昇格の脆弱性	重要	6.6	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-112800	Windows Diagnostic Policy Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95934	Windows Diagnostic Policy Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95976	Windows Diagnostic Policy Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-118142	Windows Distributed File System (DFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119917	Windows Distributed Transaction Coordinator の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119919	Windows Distributed Transaction Coordinator の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105527	Windows Encrypting File System (EFS) のサービス拒否の脆弱性	重要	5.5	なし	なし	2	サービス拒否
CVE-2026-96973	Windows Encrypting File System (EFS) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119394	Windows Enhanced Storage のリモートでコードが実行される脆弱性	重要	6.6	なし	なし	2	リモートコード実行
CVE-2026-105540	Windows Error Reporting の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-85862	Windows Error Reporting の特権の昇格の脆弱性	重要	7	なし	なし	3	特権昇格
CVE-2026-94525	Windows Error Reporting の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95947	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96153	Windows Error Reporting の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112793	Windows Event Collector Service の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-112796	Windows Event Collector Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95997	Windows Event Logging Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95977	Windows Event Viewer の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-118137	Windows FTP Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119869	Windows Failover Cluster の特権の昇格の脆弱性	重要	6.4	なし	なし	2	特権昇格
CVE-2026-113751	Windows Fast FAT Driver の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96075	Windows Feedback Hub の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-108415	Windows File Server Resource Management Service の特権の昇格の脆弱性	重要	6.8	なし	なし	3	特権昇格
CVE-2026-108416	Windows File Server Resource Management Service の特権の昇格の脆弱性	重要	6.8	なし	なし	2	特権昇格
CVE-2026-108421	Windows File Server Resource Management Service の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-113765	Windows File Server Resource Management Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-113754	Windows FileCrypt Driver の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-113757	Windows FileCrypt Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-113756	Windows FileCrypt Driver のセキュリティ機能のバイパスの脆弱性	重要	5.3	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-113755	Windows Filter Manager の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-121673	Windows Filter Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105553	Windows Filtering Platform (WFP) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112756	Windows Filtering Platform (WFP) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-88215	Windows Filtering Platform (WFP) の特権の昇格の脆弱性	重要	6.4	なし	なし	2	特権昇格
CVE-2026-119907	Windows Function Discovery Resource Publication の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-108407	Windows GDI の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-94527	Windows GDI の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-108424	Windows GDI の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-94519	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95879	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95888	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95895	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95906	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95909	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95922	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95932	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95935	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-95938	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95942	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95948	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95950	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95953	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-95966	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95971	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95973	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95974	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95983	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-95991	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96122	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96124	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96126	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-96160	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96168	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96171	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119841	Windows Graphics Kernel の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-88217	Windows Graphics Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-95946	Windows Graphics Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-96048	Windows Graphics Kernel の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-96133	Windows Graphics Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-96137	Windows Graphics Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-96144	Windows Graphics Kernel の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-119992	Windows HTTP.sys の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格
CVE-2026-95923	Windows HTTP.sys の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119385	Windows Hyper-V のサービス拒否の脆弱性	重要	4.7	なし	なし	2	サービス拒否
CVE-2026-119955	Windows Hyper-V のサービス拒否の脆弱性	重要	6	なし	なし	2	サービス拒否
CVE-2026-95913	Windows Hyper-V のサービス拒否の脆弱性	重要	5.9	なし	なし	2	サービス拒否
CVE-2026-96965	Windows Hyper-V のサービス拒否の脆弱性	重要	5.3	なし	なし	2	サービス拒否
CVE-2026-119391	Windows Hyper-V の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-119826	Windows Hyper-V の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95910	Windows Hyper-V のセキュリティ機能のバイパスの脆弱性	重要	6.7	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-119959	Windows Hyper-V のなりすましの脆弱性	重要	5.3	なし	なし	2	なりすまし
CVE-2026-122169	Windows IKE Extension のなりすましの脆弱性	重要	7.5	なし	なし	2	なりすまし
CVE-2026-119871	Windows IP Translation Configuration Service の特権の昇格の脆弱性	重要	6.4	なし	なし	2	特権昇格
CVE-2026-122163	Windows Image Acquisition 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	2	リモートコード実行
CVE-2026-96164	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	2	リモートコード実行
CVE-2026-119862	Windows Input System の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-119916	Windows Input System の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105501	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-105507	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105532	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105543	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105545	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-113847	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119398	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格
CVE-2026-119399	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119831	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119852	Windows Installer の特権の昇格の脆弱性	重要	6.7	なし	なし	2	特権昇格
CVE-2026-119865	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119892	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-119903	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-119929	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95951	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96004	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96008	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-96019	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96026	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96027	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96028	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96029	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96035	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96036	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96046	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96047	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96060	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96061	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96062	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96073	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96085	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96152	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112789	Windows Installer の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-119838	Windows Installer の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-119887	Windows Installer の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-119867	Windows Installer のセキュリティ機能のバイパスの脆弱性	重要	5.3	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-96093	Windows Internet (wininet.dll) の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-118124	Windows Internet Connection Sharing (ICS) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119859	Windows Internet Connection Sharing (ICS) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119860	Windows Internet Connection Sharing (ICS) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119861	Windows Internet Connection Sharing (ICS) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-122179	Windows Internet Connection Sharing (ICS) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119909	Windows Internet Information Services のサービス拒否の脆弱性	重要	5.9	なし	なし	2	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-119936	Windows Internet Information Services のサービス拒否の脆弱性	重要	5.9	なし	なし	2	サービス拒否
CVE-2026-105584	Windows Inventory Backup の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-112985	Windows JScript 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	2	リモートコード実行
CVE-2026-119940	Windows Kerberos のサービス拒否の脆弱性	重要	6.5	なし	なし	3	サービス拒否
CVE-2026-70240	Windows Kerberos のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-96082	Windows Kerberos のサービス拒否の脆弱性	重要	6.5	なし	なし	2	サービス拒否
CVE-2026-119847	Windows Kerberos の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-122164	Windows Kerberos の特権の昇格の脆弱性	重要	8	なし	なし	3	特権昇格
CVE-2026-85844	Windows Kerberos の特権の昇格の脆弱性	重要	9.8	なし	なし	2	特権昇格
CVE-2026-105504	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105513	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105566	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-108403	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-109473	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-112790	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	3	特権昇格
CVE-2026-112802	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112805	Windows Kernel の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-112969	Windows Kernel の特権の昇格の脆弱性	重要	6.6	なし	なし	2	特権昇格
CVE-2026-114170	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-118143	Windows Kernel の特権の昇格の脆弱性	重要	6.8	なし	なし	3	特権昇格
CVE-2026-119868	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119884	Windows Kernel の特権の昇格の脆弱性	重要	6.8	なし	なし	3	特権昇格
CVE-2026-119912	Windows Kernel の特権の昇格の脆弱性	重要	6.7	なし	なし	2	特権昇格
CVE-2026-119918	Windows Kernel の特権の昇格の脆弱性	重要	6.8	なし	なし	2	特権昇格
CVE-2026-119935	Windows Kernel の特権の昇格の脆弱性	重要	6.8	なし	なし	3	特権昇格
CVE-2026-119965	Windows Kernel の特権の昇格の脆弱性	重要	6.4	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-122183	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-94514	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格
CVE-2026-95905	Windows Kernel の特権の昇格の脆弱性	重要	6.8	なし	なし	2	特権昇格
CVE-2026-95988	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-96031	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96052	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	3	特権昇格
CVE-2026-96129	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	3	特権昇格
CVE-2026-105552	Windows Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-119857	Windows Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-96058	Windows Kernel の情報漏洩の脆弱性	重要	4.6	なし	なし	2	情報漏洩
CVE-2026-112973	Windows Kernel のセキュリティ機能のバイパスの脆弱性	重要	7.1	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-119397	Windows Kernel Transaction Manager の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-94522	Windows Kernel Transaction Manager の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-122297	Windows Kernel Transaction Manager の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-94517	Windows Kernel Transaction Manager の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-96139	Windows Kernel-Mode Drivers の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-88230	Windows LUA File Virtualization Filter Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-96117	Windows LUA File Virtualization Filter Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-113766	Windows Language Experience Service の改ざんの脆弱性	重要	3.3	なし	なし	2	改ざん
CVE-2026-108402	Windows Layer-2 Bridge Network Driver のサービス拒否の脆弱性	重要	5.3	なし	なし	3	サービス拒否
CVE-2026-116707	Windows Link Layer Topology Discovery Protocol の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-116706	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	7.5	なし	なし	2	リモートコード実行
CVE-2026-88244	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	7.5	なし	なし	3	リモートコード実行
CVE-2026-112975	Windows Link-Layer Discovery Protocol (LLDP) のサービス拒否の脆弱性	重要	5.3	なし	なし	2	サービス拒否
CVE-2026-113816	Windows Link-Layer Discovery Protocol (LLDP) の特権の昇格の脆弱性	重要	4.1	なし	なし	3	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-112807	Windows Local Security Authority Subsystem Service (LSASS) のサービス拒否の脆弱性	重要	6.5	なし	なし	2	サービス拒否
CVE-2026-70231	Windows Local Security Authority Subsystem Service (LSASS) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-85801	Windows Local Security Authority Subsystem Service (LSASS) の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-88227	Windows Local Security Authority Subsystem Service (LSASS) の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-88228	Windows Local Security Authority Subsystem Service (LSASS) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96016	Windows Local Security Authority Subsystem Service (LSASS) の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96066	Windows Local Security Authority Subsystem Service (LSASS) の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95876	Windows Local Session Manager (LSM) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105565	Windows MIDI Service Module の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105574	Windows MIDI Service Module の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119901	Windows MIDI Service Module の特権の昇格の脆弱性	重要	6.4	なし	なし	2	特権昇格
CVE-2026-105503	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105524	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-105546	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112814	Windows Management Instrumentation の特権の昇格の脆弱性	重要	5.5	なし	なし	2	特権昇格
CVE-2026-95920	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-108410	Windows Management Instrumentation の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-112965	Windows Management Instrumentation の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-105580	Windows Management Instrumentation 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	2	リモートコード実行
CVE-2026-119836	Windows Management Services の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-122182	Windows Maps の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-88229	Windows Media Player 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	2	リモートコード実行
CVE-2026-105515	Windows Message Queuing のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-119848	Windows Message Queuing のサービス拒否の脆弱性	重要	5.3	なし	なし	2	サービス拒否
CVE-2026-118125	Windows Message Queuing の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-118126	Windows Message Queuing の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-119833	Windows Message Queuing の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119816	Windows Microsoft Account Sign-in Assistant の特権の昇格の脆弱性	重要	7.8	なし	なし	3	特権昇格
CVE-2026-119921	Windows Microsoft Account Sign-in Assistant の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119944	Windows Mobile Device Management の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-112987	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-113820	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96184	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-102219	Windows Modern Device Management (MDM) 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	2	リモートコード実行
CVE-2026-119945	Windows Modern Device Management (MDM) 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	2	リモートコード実行
CVE-2026-118220	Windows Multiple Provider Router の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-100223	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119900	Windows NTFS の特権の昇格の脆弱性	重要	7.3	なし	なし	2	特権昇格
CVE-2026-119933	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-105542	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	3	リモートコード実行
CVE-2026-113848	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	3	リモートコード実行
CVE-2026-102200	Windows NTFS の改ざんの脆弱性	重要	4.7	なし	なし	2	改ざん
CVE-2026-113844	Windows NTFS の改ざんの脆弱性	重要	5.5	なし	なし	2	改ざん
CVE-2026-121680	Windows NTLM のなりすましの脆弱性	重要	7.5	なし	なし	2	なりすまし
CVE-2026-105551	Windows NetBIOS の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-112798	Windows NetBIOS の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格
CVE-2026-119873	Windows NetBIOS の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96971	Windows NetBIOS の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-88212	Windows Network Address Translation (NAT) 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	3	リモートコード実行
CVE-2026-105525	Windows Network Connection Broker の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-108406	Windows Network Connection Broker の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119821	Windows Network Connection Broker の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-118736	Windows Network File System の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-105587	Windows OLE DB の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95933	Windows OLE の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96110	Windows OLE の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-112760	Windows Overlay Filter の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112813	Windows Overlay Filter の特権の昇格の脆弱性	重要	4.7	なし	なし	2	特権昇格
CVE-2026-119822	Windows Overlay Filter の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-121670	Windows Overlay Filter の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-108409	Windows Overlay Filter の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-112750	Windows Overlay Filter の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-96981	Windows PCI Bus Driver の特権の昇格の脆弱性	重要	6.4	なし	なし	2	特権昇格
CVE-2026-96992	Windows PCI Bus Driver の特権の昇格の脆弱性	重要	6.4	なし	なし	3	特権昇格
CVE-2026-105018	Windows Partition Management Driver の特権の昇格の脆弱性	重要	6.6	なし	なし	2	特権昇格
CVE-2026-88220	Windows Performance Counters の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-113768	Windows Performance Counters 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	2	リモートコード実行
CVE-2026-95975	Windows Performance Counters 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	2	リモートコード実行
CVE-2026-96993	Windows Performance Monitor 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	2	リモートコード実行
CVE-2026-96107	Windows Phone Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105511	Windows Point-to-Point Protocol over Ethernet (PPPoE) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-118123	Windows Point-to-Point Protocol over Ethernet (PPPoE) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-124225	Windows PowerShell 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	2	リモートコード実行
CVE-2026-105567	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112752	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112762	Windows Print Spooler Components の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-112765	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112791	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-112792	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112797	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112811	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-112976	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112978	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112980	Windows Print Spooler Components の特権の昇格の脆弱性	重要	6.7	なし	なし	2	特権昇格
CVE-2026-112981	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-113770	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119913	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119939	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119950	Windows Print Spooler Components の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-105531	Windows Print Spooler Components の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-112806	Windows Print Spooler Components の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-112808	Windows Print Spooler Components の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-119898	Windows PrintWorkflowUserSvc の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119928	Windows PrintWorkflowUserSvc の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-123388	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-88247	Windows Program Compatibility Assistant Service の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-112799	Windows Projected File System の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-108414	Windows Projected File System Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-113764	Windows Projected File System の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-96023	Windows Push Notification Core の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95881	Windows Push Notifications の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112755	Windows RNDIS の特権の昇格の脆弱性	重要	6.8	なし	なし	3	特権昇格
CVE-2026-113772	Windows Redirected Drive Buffering の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-108412	Windows Redirected Drive Buffering System の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-119396	Windows Remote Access API の改ざんの脆弱性	重要	6.5	なし	なし	2	改ざん
CVE-2026-113843	Windows Remote Access Connection Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112751	Windows Remote Assistance の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119839	Windows Remote Desktop Client の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-108417	Windows Remote Desktop Client の情報漏洩の脆弱性	重要	6.5	なし	なし	3	情報漏洩
CVE-2026-108418	Windows Remote Desktop Client の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-108419	Windows Remote Desktop Client の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-121677	Windows Remote Desktop Client の情報漏洩の脆弱性	重要	6.5	なし	なし	2	情報漏洩
CVE-2026-121678	Windows Remote Desktop Client の情報漏洩の脆弱性	重要	5.3	なし	なし	3	情報漏洩
CVE-2026-95908	Windows Remote Desktop Client の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-119932	Windows Remote Desktop のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-122166	Windows Remote Desktop Services の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119882	Windows Remote Desktop Services の情報漏洩の脆弱性	重要	5.3	なし	なし	2	情報漏洩
CVE-2026-69327	Windows Remote Desktop Services 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	2	リモートコード実行
CVE-2026-69565	Windows Remote Desktop Services 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	2	リモートコード実行
CVE-2026-105509	Windows Resilient File System (ReFS) の特権の昇格の脆弱性	重要	7	なし	なし	3	特権昇格
CVE-2026-119386	Windows Resilient File System (ReFS) の特権の昇格の脆弱性	重要	7	なし	なし	3	特権昇格
CVE-2026-96081	Windows Rich Text Edit Control 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	2	リモートコード実行
CVE-2026-112812	Windows SMB Client の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112970	Windows SMB Client の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格
CVE-2026-112971	Windows SMB Client の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119870	Windows SMB Client の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119988	Windows SMB 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	2	リモートコード実行
CVE-2026-122176	Windows SMB 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	2	リモートコード実行
CVE-2026-112972	Windows SMBv3 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	2	リモートコード実行
CVE-2026-119906	Windows Sandbox の特権の昇格の脆弱性	重要		なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-112757	Windows Secure Kernel Mode の情報漏洩の脆弱性	重要	6	なし	なし	2	情報漏洩
CVE-2026-105561	Windows Secure Socket Tunneling Protocol (SSTP) のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-105510	Windows Secure Socket Tunneling Protocol (SSTP) の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112795	Windows Security Account Manager のサービス拒否の脆弱性	重要	6.5	なし	なし	2	サービス拒否
CVE-2026-112966	Windows Security Account Manager のサービス拒否の脆弱性	重要	7.5	なし	なし	2	サービス拒否
CVE-2026-122474	Windows Security Account Manager Remote Protocol のセキュリティ機能のバイパスの脆弱性	重要	5.9	なし	なし	2	セキュリティ機能のバイパス
CVE-2026-113842	Windows Security Center の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-88241	Windows Sensor Data Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-112989	Windows Servicing Stack Updates の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105547	Windows Setup and Deployment の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119914	Windows Setup and Deployment の特権の昇格の脆弱性	重要	6.7	なし	なし	2	特権昇格
CVE-2026-119817	Windows Shell の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-97013	Windows Shell の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-102868	Windows Shell の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-105506	Windows Shell の情報漏洩の脆弱性	重要	5	なし	なし	2	情報漏洩
CVE-2026-119938	Windows Shell 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	2	リモートコード実行
CVE-2026-85907	Windows Simple Search and Discovery Protocol (SSDP) Service の特権の昇格の脆弱性	重要	4.4	なし	なし	2	特権昇格
CVE-2026-112794	Windows Smart Card の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-118144	Windows Smart Card の特権の昇格の脆弱性	重要	6.6	なし	なし	2	特権昇格
CVE-2026-119383	Windows Smart Card の特権の昇格の脆弱性	重要	6.6	なし	なし	3	特権昇格
CVE-2026-119835	Windows Smart Card の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95968	Windows Smart Card の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105549	Windows Smart Card の情報漏洩の脆弱性	重要	4.3	なし	なし	3	情報漏洩
CVE-2026-112979	Windows State Repository Service の改ざんの脆弱性	重要	5.5	なし	なし	2	改ざん
CVE-2026-95998	Windows StateRepository API の改ざんの脆弱性	重要	4.4	なし	なし	2	改ざん
CVE-2026-105529	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-119389	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格
CVE-2026-95889	Windows Storage の特権の昇格の脆弱性	重要	6.6	なし	なし	2	特権昇格
CVE-2026-105534	Windows Storage 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	2	リモートコード実行
CVE-2026-105024	Windows Storage Spaces Controller の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119392	Windows Storage Spaces Controller の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-119851	Windows Storage Spaces Controller の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-113814	Windows Storage Spaces Controller 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	2	リモートコード実行
CVE-2026-119908	Windows Storage Spaces Controller 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	2	リモートコード実行
CVE-2026-122475	Windows Storage Spaces Controller 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	2	リモートコード実行
CVE-2026-119830	Windows Storport Miniport Driver の特権の昇格の脆弱性	重要	6.8	なし	なし	2	特権昇格
CVE-2026-119885	Windows Storport Miniport Driver の特権の昇格の脆弱性	重要	6.8	なし	なし	2	特権昇格
CVE-2026-119875	Windows Storport Miniport Driver の情報漏洩の脆弱性	重要	4	なし	なし	2	情報漏洩
CVE-2026-119823	Windows Storport Miniport Driver 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	2	リモートコード実行
CVE-2026-119834	Windows Subsystem for Linux の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119846	Windows Subsystem for Linux の特権の昇格の脆弱性	重要	7.8	なし	なし	3	特権昇格
CVE-2026-88237	Windows Subsystem for Linux の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-105530	Windows System Events Broker の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-96077	Windows TCP/IP のサービス拒否の脆弱性	重要	7.5	なし	なし	1	サービス拒否
CVE-2026-96102	Windows TCP/IP の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96969	Windows TCP/IP の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112759	Windows Task Scheduler の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格
CVE-2026-122174	Windows Task Scheduler の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-88233	Windows Task Scheduler の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95894	Windows Task Scheduler の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96053	Windows Task Scheduler の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96845	Windows Task Scheduler の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-108413	Windows Telephony Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-116700	Windows Telephony Service の特権の昇格の脆弱性	重要	6.6	なし	なし	2	特権昇格
CVE-2026-119886	Windows Telephony Service の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-108408	Windows Telephony Service の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-119818	Windows Text Services Framework の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-119925	Windows Text Services Framework の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-119931	Windows Text Services Framework の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96022	Windows Text Services Framework の情報漏洩の脆弱性	重要	5.6	なし	なし	2	情報漏洩
CVE-2026-119829	Windows USB Audio Class driver (usbaudio.sys) の特権の昇格の脆弱性	重要	6.8	なし	なし	2	特権昇格
CVE-2026-112764	Windows USB Driver の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119872	Windows USB Driver の特権の昇格の脆弱性	重要	6.4	なし	なし	2	特権昇格
CVE-2026-122167	Windows USB Driver の特権の昇格の脆弱性	重要	6.8	なし	なし	2	特権昇格
CVE-2026-95872	Windows USB Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96005	Windows USB Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96051	Windows USB Driver の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96055	Windows USB Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96056	Windows USB Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-96057	Windows USB Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95902	Windows USB Hub Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95999	Windows USB Hub Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	3	特権昇格
CVE-2026-96041	Windows USB Hub Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-119876	Windows USB Scanner Driver の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-112984	Windows USB Video Driver の特権の昇格の脆弱性	重要	6.6	なし	なし	2	特権昇格
CVE-2026-112990	Windows USB Video Driver の特権の昇格の脆弱性	重要	4.7	なし	なし	3	特権昇格
CVE-2026-95961	Windows USB Video Driver の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95965	Windows USB Video Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-97000	Windows USM Communication Manager の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119837	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-119840	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	6.3	なし	なし	2	特権昇格
CVE-2026-122984	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	2	特権昇格
CVE-2026-122162	Windows Update Stack の情報漏洩の脆弱性	重要	5.5	なし	なし	2	情報漏洩
CVE-2026-95987	Windows User Manager Service の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96037	Windows User Manager Service の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95962	Windows Virtual Filtering Platform (VFP) のリモートでコードが実行される脆弱性	重要	9	なし	なし	2	リモートコード実行
CVE-2026-96086	Windows WLAN Service のサービス拒否の脆弱性	重要	6.5	なし	なし	2	サービス拒否
CVE-2026-105028	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-119827	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-119899	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-122170	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-108423	Windows WinHTTP の情報漏洩の脆弱性	重要	4.7	なし	なし	2	情報漏洩
CVE-2026-105589	Windows Wireless Networking の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-113760	Windows XWizard Framework の特権の昇格の脆弱性	重要	8.8	なし	なし	2	特権昇格
CVE-2026-112801	Windows eSCL Scanner の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-95956	Windows eSCL Scanner 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	2	リモートコード実行
CVE-2026-112766	Windows exFAT File System の特権の昇格の脆弱性	重要	7	なし	なし	3	特権昇格
CVE-2026-112804	Windows exFAT File System の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-122177	Windows iSCSI の特権の昇格の脆弱性	重要	7.5	なし	なし	2	特権昇格
CVE-2026-95898	Windows iSCSI の特権の昇格の脆弱性	重要	7.8	なし	なし	2	特権昇格
CVE-2026-88231	Windows iSCSI の情報漏洩の脆弱性	重要	5.7	なし	なし	2	情報漏洩
CVE-2026-105518	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	2	リモートコード実行
CVE-2026-88234	Windows iSCSI 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	2	リモートコード実行
CVE-2026-83684	Windows iSCSI Target Service の情報漏洩の脆弱性	重要	7.5	なし	なし	2	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	XI	種類
CVE-2026-105522	Winlogon の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-83563	Winlogon の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-105526	Winsock の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-96994	Winsock の特権の昇格の脆弱性	重要	7	なし	なし	2	特権昇格
CVE-2026-95874	Xbox Gaming Services の特権の昇格の脆弱性	重要	7.8	なし	なし	1	特権昇格
CVE-2026-95989	vhdmp.sys の特権の昇格の脆弱性	重要	7	なし	なし	1	特権昇格

出典：Zero Day Initiative – The November 2026 Security Update Review