CVE	タイトル	深刻度	CVSS	公開	悪用	XI	種別
CVE-2026-41091	Microsoft Defender の特権の昇格の脆弱性	重要	7.8	はい	はい	0	EoP
CVE-2026-49160	HTTP.sys のサービス拒否の脆弱性	重要	7.5	はい	いいえ	1	DoS
CVE-2026-50507	Windows BitLocker のセキュリティ機能のバイパスの脆弱性	重要	6.8	はい	いいえ	1	SFB
CVE-2026-45586	Windows Collaborative Translation Framework（CTFMON）の特権の昇格の脆弱性	重要	7.8	はい	いいえ	1	EoP
CVE-2025-10263 *	ARM: CVE-2025-10263 TLBIの完了によって、影響を受けるメモリアクセスの完了が保証されない場合がある [kerr	緊急	9.3	いいえ	いいえ	2	EoP
CVE-2026-48567	Azure HorizonDB の特権の昇格の脆弱性	緊急	10	いいえ	いいえ	N/A	EoP
CVE-2026-32193	Azure Kubernetes Service（AKS）のリモートでコードが実行される脆弱性	緊急	8.8	いいえ	いいえ	3	RCE
CVE-2026-47644	Copilot Chat（Microsoft Edge）の情報漏えいの脆弱性	緊急	6.5	いいえ	いいえ	2	Info
CVE-2026-44815	DHCP Client Service のリモートでコードが実行される脆弱性	緊急	9.8	いいえ	いいえ	2	RCE
CVE-2026-47291	HTTP.sys のリモートでコードが実行される脆弱性	緊急	9.8	いいえ	いいえ	1	RCE
CVE-2026-42824	M365 Copilot の情報漏えいの脆弱性	緊急	6.5	いいえ	いいえ	N/A	Info
CVE-2026-45476	Microsoft Azure Network Adapter の特権の昇格の脆弱性	緊急	8.2	いいえ	いいえ	2	EoP
CVE-2026-44810	Microsoft Cryptographic Services の特権の昇格の脆弱性	緊急	8.4	いいえ	いいえ	2	EoP
CVE-2026-48579	Microsoft Exchange Online の情報漏えいの脆弱性	緊急	9.1	いいえ	いいえ	N/A	Info
CVE-2026-47655	Microsoft Graph の情報漏えいの脆弱性	緊急	6.5	いいえ	いいえ	N/A	Info
CVE-2026-45497	Microsoft M365 Copilot のリモートでコードが実行される脆弱性	緊急	7.7	いいえ	いいえ	N/A	RCE
CVE-2026-45460	Microsoft Office の情報漏えいの脆弱性	緊急	4.7	いいえ	いいえ	3	Info
CVE-2026-45472	Microsoft Office のリモートでコードが実行される脆弱性	緊急	8.4	いいえ	いいえ	2	RCE
CVE-2026-45474	Microsoft Office のリモートでコードが実行される脆弱性	緊急	8.4	いいえ	いいえ	2	RCE
CVE-2026-45461	Microsoft Office のリモートでコードが実行される脆弱性	緊急	8.4	いいえ	いいえ	2	RCE
CVE-2026-45463	Microsoft Office のリモートでコードが実行される脆弱性	緊急	8.4	いいえ	いいえ	2	RCE
CVE-2026-45456	Microsoft Outlook および Word のリモートでコードが実行される脆弱性	緊急	8.4	いいえ	いいえ	2	RCE
CVE-2026-45458	Microsoft Outlook および Word のリモートでコードが実行される脆弱性	緊急	8.4	いいえ	いいえ	2	RCE
CVE-2026-47635	Microsoft Outlook および Word のリモートでコードが実行される脆弱性	緊急	8.4	いいえ	いいえ	2	RCE
CVE-2026-26142	Nuance PowerScribe のリモートでコードが実行される脆弱性	緊急	9.8	いいえ	いいえ	2	RCE
CVE-2026-47289	Remote Desktop Client のリモートでコードが実行される脆弱性	緊急	8.8	いいえ	いいえ	2	RCE
CVE-2026-47654	Remote Desktop Client のリモートでコードが実行される脆弱性	緊急	7.5	いいえ	いいえ	3	RCE
CVE-2026-48563	Remote Desktop Client のリモートでコードが実行される脆弱性	緊急	7.5	いいえ	いいえ	2	RCE
CVE-2026-42992	Remote Desktop Client のリモートでコードが実行される脆弱性	緊急	7.5	いいえ	いいえ	2	RCE
CVE-2026-44799	Remote Desktop Client のリモートでコードが実行される脆弱性	緊急	7.5	いいえ	いいえ	2	RCE
CVE-2026-44801	Remote Desktop Client のリモートでコードが実行される脆弱性	緊急	7.5	いいえ	いいえ	2	RCE
CVE-2026-42985	Remote Desktop Client のリモートでコードが実行される脆弱性	緊急	8.8	いいえ	いいえ	1	RCE
CVE-2026-45648	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	いいえ	いいえ	3	RCE
CVE-2026-42987	Windows Deployment Services（WDS）のリモートでコードが実行される脆弱性	緊急	8.1	いいえ	いいえ	2	RCE
CVE-2026-33828	Windows Device Health Attestation（DHA）の特権の昇格の脆弱性	緊急	7.8	いいえ	いいえ	3	EoP
CVE-2026-44803	Windows Graphics Component のリモートでコードが実行される脆弱性	緊急	7.8	いいえ	いいえ	1	RCE
CVE-2026-44812	Windows Graphics Component のリモートでコードが実行される脆弱性	緊急	7.8	いいえ	いいえ	1	RCE

CVE-2026-45607	Windows Hyper-V のリモートでコードが実行される脆弱性	緊急	8.4	いいえ	いいえ	2	RCE
CVE-2026-45641	Windows Hyper-V のリモートでコードが実行される脆弱性	緊急	8.4	いいえ	いいえ	2	RCE
CVE-2026-47652	Windows Hyper-V のリモートでコードが実行される脆弱性	緊急	8.2	いいえ	いいえ	2	RCE
CVE-2026-47288	Windows Kerberos キー配布センター（KDC）のリモートでコードが実行される脆弱性	緊急	7.1	いいえ	いいえ	3	RCE
CVE-2026-45657	Windows Kernel のリモートでコードが実行される脆弱性	緊急	9.8	いいえ	いいえ	2	RCE
CVE-2026-48574	Windows Media のリモートでコードが実行される脆弱性	緊急	7.8	いいえ	いいえ	2	RCE
CVE-2026-45490	.NET SDK の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-45491	.NET の改ざんの脆弱性	重要	6.2	いいえ	いいえ	3	Tampering
CVE-2026-45591	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	いいえ	いいえ	2	DoS
CVE-2026-47643	Azure Stack Edge のリモートでコードが実行される脆弱性	重要	9.8	いいえ	いいえ	3	RCE
CVE-2026-41098	Azure Stack Edge のなりすましの脆弱性	重要	8.4	いいえ	いいえ	2	Spoofing
CVE-2026-45642	Microsoft Azure Attestation サービスおよび Device Health Attestation サービスのなりすましの脆弱性	重要	3.9	いいえ	いいえ	2	Spoofing
CVE-2026-45650	Microsoft Bing Search のなりすましの脆弱性	重要	4.3	いいえ	いいえ	2	Spoofing
CVE-2026-45637	Microsoft DWM Core Library の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-45647	Microsoft Defender for Endpoint for Mac の特権の昇格の脆弱性	重要	5.5	いいえ	いいえ	2	EoP
CVE-2026-40371	Microsoft Dynamics 365（オンプレミス）の特権の昇格の脆弱性	重要	8.8	いいえ	いいえ	2	EoP
CVE-2026-44822	Microsoft Excel の情報漏えいの脆弱性	重要	8.2	いいえ	いいえ	3	Info
CVE-2026-45455	Microsoft Excel の情報漏えいの脆弱性	重要	3.3	いいえ	いいえ	2	Info
CVE-2026-45469	Microsoft Excel のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-44817	Microsoft Excel のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	3	RCE
CVE-2026-44818	Microsoft Excel のリモートでコードが実行される脆弱性	重要	7	いいえ	いいえ	2	RCE
CVE-2026-44820	Microsoft Excel のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-44823	Microsoft Excel のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-45459	Microsoft Excel のセキュリティ機能のバイパスの脆弱性	重要	3.3	いいえ	いいえ	2	SFB
CVE-2026-45504	Microsoft Exchange Server の特権の昇格の脆弱性	重要	8.8	いいえ	いいえ	3	EoP
CVE-2026-45502	Microsoft Exchange Server の情報漏えいの脆弱性	重要	5	いいえ	いいえ	3	Info
CVE-2026-45503	Microsoft Exchange Server の情報漏えいの脆弱性	重要	8.1	いいえ	いいえ	3	Info
CVE-2026-45583	Microsoft Exchange Server のリモートでコードが実行される脆弱性	重要	7.5	いいえ	いいえ	2	RCE
CVE-2026-45500	Microsoft Exchange Server のなりすましの脆弱性	重要	6.1	いいえ	いいえ	2	Spoofing
CVE-2026-45501	Microsoft Exchange Server のなりすましの脆弱性	重要	6.5	いいえ	いいえ	2	Spoofing
CVE-2026-47631	Microsoft Exchange Server のなりすましの脆弱性	重要	8.1	いいえ	いいえ	2	Spoofing
CVE-2026-42986	Microsoft Graphics Component の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	1	EoP
CVE-2026-41092	Microsoft Kinect の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-45644	Microsoft Live Share Canvas SDK の特権の昇格の脆弱性	重要	8	いいえ	いいえ	2	EoP
CVE-2026-47293	Microsoft Office Click-To-Run の特権の昇格の脆弱性	重要	7	いいえ	いいえ	2	EoP
CVE-2026-45485	Microsoft Office の情報漏えいの脆弱性	重要	3.3	いいえ	いいえ	2	Info
CVE-2026-44821	Microsoft Office の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-45483	Microsoft Office Project Server のなりすましの脆弱性	重要	4.6	いいえ	いいえ	2	Spoofing

CVE-2026-45475	Microsoft Office のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-44819	Microsoft Office のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-44824	Microsoft Office のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-45645	Microsoft Office のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-49161	Microsoft PC Manager 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	3	SFB
CVE-2026-42902	Microsoft PowerToys の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-45484	Microsoft SharePoint の特権の昇格の脆弱性	重要	8.8	いいえ	いいえ	2	EoP
CVE-2026-45454	Microsoft SharePoint のリモートでコードが実行される脆弱性	重要	6.5	いいえ	いいえ	2	RCE
CVE-2026-47298	Microsoft SharePoint Server のリモートでコードが実行される脆弱性	重要	8	いいえ	いいえ	2	RCE
CVE-2026-45467	Microsoft SharePoint Server のなりすましの脆弱性	重要	4.6	いいえ	いいえ	2	Spoofing
CVE-2026-45468	Microsoft SharePoint Server のなりすましの脆弱性	重要	4.6	いいえ	いいえ	2	Spoofing
CVE-2026-45479	Microsoft SharePoint Server のなりすましの脆弱性	重要	4.6	いいえ	いいえ	2	Spoofing
CVE-2026-45453	Microsoft SharePoint Server のなりすましの脆弱性	重要	5.4	いいえ	いいえ	2	Spoofing
CVE-2026-47636	Microsoft SharePoint Server のなりすましの脆弱性	重要	5.4	いいえ	いいえ	2	Spoofing
CVE-2026-47637	Microsoft SharePoint Server のなりすましの脆弱性	重要	4.6	いいえ	いいえ	2	Spoofing
CVE-2026-47638	Microsoft SharePoint Server のなりすましの脆弱性	重要	4.6	いいえ	いいえ	2	Spoofing
CVE-2026-47639	Microsoft SharePoint Server のなりすましの脆弱性	重要	5.4	いいえ	いいえ	3	Spoofing
CVE-2026-47641	Microsoft SharePoint Server のなりすましの脆弱性	重要	4.6	いいえ	いいえ	2	Spoofing
CVE-2026-33113	Microsoft SharePoint Server のなりすましの脆弱性	重要	5.4	いいえ	いいえ	2	Spoofing
CVE-2026-45462	Microsoft SharePoint Server のなりすましの脆弱性	重要	4.6	いいえ	いいえ	2	Spoofing
CVE-2026-45464	Microsoft SharePoint Server のなりすましの脆弱性	重要	5.4	いいえ	いいえ	2	Spoofing
CVE-2026-45465	Microsoft SharePoint Server のなりすましの脆弱性	重要	5.4	いいえ	いいえ	2	Spoofing
CVE-2026-47634	Microsoft SharePoint Server のなりすましの脆弱性	重要	7.3	いいえ	いいえ	1	Spoofing
CVE-2026-47640	Microsoft SharePoint Server のなりすましの脆弱性	重要	4.6	いいえ	いいえ	3	Spoofing
CVE-2026-45481	Microsoft SharePoint Server のなりすましの脆弱性	重要	7.3	いいえ	いいえ	1	Spoofing
CVE-2026-48560	Microsoft SharePoint Server のなりすましの脆弱性	重要	5.4	いいえ	いいえ	2	Spoofing
CVE-2026-48562	Microsoft SharePoint Server のなりすましの脆弱性	重要	4.6	いいえ	いいえ	2	Spoofing
CVE-2026-42835	Microsoft Teams for Android の情報漏えいの脆弱性	重要	8.1	いいえ	いいえ	2	Info
CVE-2026-45606	Microsoft UxTheme Library（uxtheme.dll）のサービス拒否の脆弱性	重要	5.5	いいえ	いいえ	2	DoS
CVE-2026-45482	Microsoft Visual Studio Code CoPilot Chat 拡張機能のセキュリティ機能のバイパスの脆弱性	重要	8.4	いいえ	いいえ	2	SFB
CVE-2026-45466	Microsoft Word の情報漏えいの脆弱性	重要	3.3	いいえ	いいえ	3	Info
CVE-2026-45471	Microsoft Word のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-45486	Microsoft Word のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-45643	Microsoft Word のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-45457	Microsoft Word のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-42980	NT OS Kernel の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	1	EoP
CVE-2026-42916	NT OS Kernel の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-45649	Office for Android のなりすましの脆弱性	重要	7.1	いいえ	いいえ	3	Spoofing

CVE-2026-47653	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	いいえ	いいえ	3	RCE
CVE-2026-42909	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	いいえ	いいえ	3	RCE
CVE-2026-42913	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	いいえ	いいえ	3	RCE
CVE-2026-42993	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	いいえ	いいえ	2	RCE
CVE-2026-45588	Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	7.9	いいえ	いいえ	2	SFB
CVE-2026-48568	Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	7.9	いいえ	いいえ	2	SFB
CVE-2026-48570	Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	7.9	いいえ	いいえ	2	SFB
CVE-2026-48573	Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	7.9	いいえ	いいえ	2	SFB
CVE-2026-48575	Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	7.9	いいえ	いいえ	2	SFB
CVE-2026-48576	Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	7.9	いいえ	いいえ	2	SFB
CVE-2026-48578	Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	7.9	いいえ	いいえ	2	SFB
CVE-2026-45654	Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	7.9	いいえ	いいえ	2	SFB
CVE-2026-45656	UEFI Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	7.8	いいえ	いいえ	2	SFB
CVE-2026-8863	UEFI Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	7.8	いいえ	いいえ	2	SFB
CVE-2026-40376	Visual Studio Code の特権の昇格の脆弱性	重要	7.5	いいえ	いいえ	2	EoP
CVE-2026-47281	Visual Studio Code の特権の昇格の脆弱性	重要	9.6	いいえ	いいえ	3	EoP
CVE-2026-47284	Visual Studio Code の情報漏えいの脆弱性	重要	6.5	いいえ	いいえ	2	Info
CVE-2026-47292	Visual Studio Code MSSQL 拡張機能のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-48569	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	7.1	いいえ	いいえ	2	SFB
CVE-2026-47287	Visual Studio Code の改ざんの脆弱性	重要	6.5	いいえ	いいえ	2	Tampering
CVE-2026-42829	Windows Administrator Protection 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	2	SFB
CVE-2026-34335	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	いいえ	いいえ	3	EoP
CVE-2026-45601	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	いいえ	いいえ	2	EoP
CVE-2026-45598	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	いいえ	いいえ	2	EoP
CVE-2026-45596	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	いいえ	いいえ	2	EoP
CVE-2026-45638	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-45603	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	いいえ	いいえ	2	EoP
CVE-2026-42911	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	いいえ	いいえ	2	EoP
CVE-2026-45594	Windows Application Identity（AppID）の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-45655	Windows BitLocker 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	2	SFB
CVE-2026-45658	Windows BitLocker 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	1	SFB
CVE-2026-45640	Windows Bluetooth Port Driver の特権の昇格の脆弱性	重要	7	いいえ	いいえ	2	EoP
CVE-2026-45605	Windows Bluetooth Service の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-47656	Windows Boot Manager のセキュリティ機能のバイパスの脆弱性	重要	7.9	いいえ	いいえ	2	SFB
CVE-2026-44809	Windows Common Log File System Driver の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	3	EoP
CVE-2026-45634	Windows DHCP Client の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	3	Info
CVE-2026-45608	Windows DHCP Client の情報漏えいの脆弱性	重要	6.8	いいえ	いいえ	3	Info
CVE-2026-41108	Windows DNS Client の特権の昇格の脆弱性	重要	7	いいえ	いいえ	3	EoP

CVE-2026-42905	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	1	EoP
CVE-2026-44811	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-44808	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-44807	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-42983	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-44802	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-44813	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-44804	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-48566	Windows DWM Core Library の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-44814	Windows DWM Core Library の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-45602	Windows Dynamic Host Configuration Protocol（DHCP）の改ざんの脆弱性	重要	9.1	いいえ	いいえ	2	Tampering
CVE-2026-42836	Windows Function Discovery Service（fdwsd.dll）の特権の昇格の脆弱性	重要	7	いいえ	いいえ	2	EoP
CVE-2026-42910	Windows Hotpatch Monitoring Service の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-42972	Windows Hyper-V の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-45592	Windows Internet（wininet.dll）の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	3	EoP
CVE-2026-42903	Windows Kerberos のサービス拒否の脆弱性	重要	6.5	いいえ	いいえ	3	DoS
CVE-2026-42914	Windows Kerberos のサービス拒否の脆弱性	重要	5.3	いいえ	いいえ	2	DoS
CVE-2026-48583	Windows Kernel の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-45653	Windows Kernel の特権の昇格の脆弱性	重要	7	いいえ	いいえ	3	EoP
CVE-2026-42984	Windows Kernel の特権の昇格の脆弱性	重要	7	いいえ	いいえ	3	EoP
CVE-2026-45600	Windows Kernel-Mode Driver の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	3	EoP
CVE-2026-45604	Windows Managed Installer の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-45595	Windows Mark of the Web のセキュリティ機能のバイパスの脆弱性	重要	5.4	いいえ	いいえ	2	SFB
CVE-2026-45636	Windows NTFS のリモートでコードが実行される脆弱性	重要	7.8	いいえ	いいえ	2	RCE
CVE-2026-50508	Windows NTLM のなりすましの脆弱性	重要	6.5	いいえ	いいえ	1	Spoofing
CVE-2026-48565	Windows Narrator Braille の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-44805	Windows Network Controller（NC）Host Agent のサービス拒否の脆弱性	重要	5.5	いいえ	いいえ	3	DoS
CVE-2026-42981	Windows Performance Monitor のリモートでコードが実行される脆弱性	重要	8.1	いいえ	いいえ	2	RCE
CVE-2026-42974	Windows Performance Monitor のリモートでコードが実行される脆弱性	重要	8.1	いいえ	いいえ	2	RCE
CVE-2026-45487	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	3	EoP
CVE-2026-42828	Windows Projected File System の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-42837	Windows Projected File System の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-42969	Windows Push Notification の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	3	Info
CVE-2026-42971	Windows Push Notification の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-42970	Windows Push Notification の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-42973	Windows Push Notification の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-42978	Windows Push Notifications の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	3	EoP
CVE-2026-42977	Windows Push Notifications の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	3	EoP

CVE-2026-42979	Windows Push Notifications の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	3	EoP
CVE-2026-42991	Windows Push Notifications の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	3	EoP
CVE-2026-45639	Windows Remote Desktop Protocol（RDP）の情報漏えいの脆弱性	重要	7.5	いいえ	いいえ	2	Info
CVE-2026-42908	Windows Remote Desktop Protocol（RDP）の情報漏えいの脆弱性	重要	7.5	いいえ	いいえ	2	Info
CVE-2026-45593	Windows SDK の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-42906	Windows Shell の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-42907	Windows Shell の情報漏えいの脆弱性	重要	6.5	いいえ	いいえ	2	Info
CVE-2026-47648	Windows Storage の特権の昇格の脆弱性	重要	7	いいえ	いいえ	3	EoP
CVE-2026-42915	Windows TCP/IP のサービス拒否の脆弱性	重要	5.7	いいえ	いいえ	2	DoS
CVE-2026-42904	Windows TCP/IP の特権の昇格の脆弱性	重要	9.6	いいえ	いいえ	3	EoP
CVE-2026-42968	Windows Telephony Server の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	2	Info
CVE-2026-42912	Windows Telephony Service の特権の昇格の脆弱性	重要	7	いいえ	いいえ	2	EoP
CVE-2026-45597	Windows UI Automation Manager（uiamanager.dll）の特権の昇格の脆弱性	重要	7	いいえ	いいえ	3	EoP
CVE-2026-45599	Windows UPnP Device Host のリモートでコードが実行される脆弱性	重要	8.1	いいえ	いいえ	2	RCE
CVE-2026-45635	Windows UPnP Device Host のリモートでコードが実行される脆弱性	重要	8.1	いいえ	いいえ	2	RCE
CVE-2026-40409	Windows Universal Disk Format File System Driver（UDFS）の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-40404	Windows Universal Disk Format File System Driver（UDFS）の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	2	EoP
CVE-2026-42989	Winlogon の特権の昇格の脆弱性	重要	7.8	いいえ	いいえ	1	EoP

＊ このCVEがサードパーティによってすでに公開されており、現在はMicrosoftのリリースに含められていることを示します。

† 脆弱性に完全に対処するには、追加の管理者操作が必要であることを示します。