

Microsoft 2026年10月 セキュリティアップデート

CVE 1,417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）

- * は、サードパーティが公開済みで、今回Microsoftのリリースに含まれたCVEを示します。
- ** は、Microsoftによる修正がすでに完了しており、エンドユーザによる追加対応が不要なCVEを示します。

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-96951	Windows Shell のセキュリティ機能のバイパスの脆弱性	重要	8.8	なし	あり	セキュリティ機能のバイパス
CVE-2026-108398	.NET Framework のセキュリティ機能のバイパスの脆弱性	重要	8.8	あり	なし	セキュリティ機能のバイパス
CVE-2026-92707 *	MessagePack-CSharp のサービス拒否の脆弱性	中	5.3	あり	なし	サービス拒否
CVE-2026-96222	Active Directory Federation Services (AD FS) のなりすましの脆弱性	緊急	7.4	なし	なし	なりすまし
CVE-2026-108131	Active Directory Federation Services (AD FS) のなりすましの脆弱性	緊急	7.5	なし	なし	なりすまし
CVE-2026-83943 **	Azure API Center の情報漏洩の脆弱性	緊急	8.7	なし	なし	情報漏洩
CVE-2026-77900 **	Azure App 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	リモートコード実行
CVE-2026-83947 **	Azure Event Grid のなりすましの脆弱性	緊急	7.7	なし	なし	なりすまし
CVE-2026-69435 **	Azure SRE Agent の特権の昇格の脆弱性	緊急	9.6	なし	なし	特権昇格
CVE-2026-108400	HEVC Video Extensions のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-62840	Linux Kernel の特権の昇格の脆弱性	緊急	7	なし	なし	特権昇格
CVE-2026-94510 **	Microsoft Bookings の特権の昇格の脆弱性	緊急	9.9	なし	なし	特権昇格
CVE-2026-88131 **	Microsoft Dataverse のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-105718	Microsoft 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	リモートコード実行
CVE-2026-70571	Microsoft Exchange Server のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-100215	Microsoft Graphics Component のリモートでコードが実行される脆弱性	緊急	7.8	なし	なし	リモートコード実行
CVE-2026-100209	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	リモートコード実行
CVE-2026-100210	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	リモートコード実行
CVE-2026-100211	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	リモートコード実行
CVE-2026-97739	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	リモートコード実行
CVE-2026-97745	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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-97755	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	リモートコード実行
CVE-2026-97756	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	リモートコード実行
CVE-2026-97758	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	リモートコード実行
CVE-2026-97759	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	リモートコード実行
CVE-2026-97765	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	リモートコード実行
CVE-2026-97778	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	リモートコード実行
CVE-2026-97780	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	リモートコード実行
CVE-2026-97741	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	リモートコード実行
CVE-2026-97742	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	リモートコード実行
CVE-2026-97753	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	リモートコード実行
CVE-2026-97761	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	リモートコード実行
CVE-2026-97767	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	リモートコード実行
CVE-2026-97776	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	リモートコード実行
CVE-2026-70242	Microsoft Office Outlook のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-70291	Microsoft Office Outlook のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-88156	Microsoft Office Outlook のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-97016	Microsoft Office Outlook のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-97749	Microsoft Office Outlook のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-88178	Microsoft Office PowerPoint のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-70215	Microsoft Office PowerPoint のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-88144	Microsoft Office PowerPoint のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-88207	Microsoft Office PowerPoint のリモートでコードが実行される脆弱性	緊急	7.5	なし	なし	リモートコード実行
CVE-2026-102866	Microsoft Office SharePoint の特権の昇格の脆弱性	緊急	8.1	なし	なし	特権昇格
CVE-2026-102855	Microsoft Office Visio のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-102856	Microsoft Office Visio のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-102857	Microsoft Office Visio のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70269	Microsoft Office Word のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-88185	Microsoft Office Word のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-70300	Microsoft Office Word のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-96207 **	Microsoft Partner Center の特権の昇格の脆弱性	緊急	10	なし	なし	特権昇格
CVE-2026-70147	Microsoft PostScript Printer Driver のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-70153	Microsoft PostScript Printer Driver のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-108467	Microsoft PostScript Printer Driver のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-100219	Microsoft QUIC のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-105016	Microsoft QUIC のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-96952	Microsoft Windows Media Foundation のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-108457	Microsoft Windows PDF のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-69802	Network Device Enrollment Service (NDES) のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-21413 *	Raw Image Extension のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-70229	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	8.1	なし	なし	リモートコード実行
CVE-2026-83917	Windows ALPC の特権の昇格の脆弱性	緊急	7	なし	なし	特権昇格
CVE-2026-88174	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	リモートコード実行
CVE-2026-70250	Windows DHCP Client のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-96934	Windows DHCP Server のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-88117	Windows DHCP Server のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-88119	Windows DHCP Server のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-88120	Windows DHCP Server のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-88171	Windows DHCP Server のリモートでコードが実行される脆弱性	緊急	8.1	なし	なし	リモートコード実行
CVE-2026-83934	Windows GDI+ のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-88073	Windows Graphics Kernel の特権の昇格の脆弱性	緊急	8.8	なし	なし	特権昇格
CVE-2026-108399	Windows Hyper-V の特権の昇格の脆弱性	緊急	7.2	なし	なし	特権昇格
CVE-2026-102214	Windows Hyper-V のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-105733	Windows Hyper-V のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-96913	Windows Kernel の特権の昇格の脆弱性	緊急	8.8	なし	なし	特権昇格
CVE-2026-100220	Windows Media Video Decoder のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-100202	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	9.8	なし	なし	リモートコード実行
CVE-2026-108460	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	リモートコード実行
CVE-2026-96202	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	リモートコード実行
CVE-2026-96943	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	リモートコード実行
CVE-2026-69789	Windows Reliable Multicast Transport Driver (RMCAST) のリモートでコードが実行される脆弱性	緊急	7.5	なし	なし	リモートコード実行
CVE-2026-70187	Windows Remote Desktop 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	リモートコード実行
CVE-2026-102225	Windows Text Shaping のリモートでコードが実行される脆弱性	緊急	8.8	なし	なし	リモートコード実行
CVE-2026-97814	Windows Text Shaping のリモートでコードが実行される脆弱性	緊急	9.8	なし	なし	リモートコード実行
CVE-2026-96914	Windows Virtualization-Based Security (VBS) Enclave の特権の昇格の脆弱性	緊急	8.8	なし	なし	特権昇格
CVE-2026-108130	Windows Virtualization-Based Security (VBS) Enclave の特権の昇格の脆弱性	緊急	7.8	なし	なし	特権昇格
CVE-2026-88074	Windows Virtualization-Based Security (VBS) Enclave の特権の昇格の脆弱性	緊急	7.8	なし	なし	特権昇格
CVE-2026-102211	Windows Virtualization-Based Security (VBS) Enclave の特権の昇格の脆弱性	緊急	7	なし	なし	特権昇格
CVE-2026-108471	Windows Virtualization-Based Security (VBS) Enclave の特権の昇格の脆弱性	緊急	8.8	なし	なし	特権昇格
CVE-2026-102869	.NET and Visual Studio の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-58280	.NET のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69651	.NET のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-84008	.NET のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-96958	.NET のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-96959	.NET のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-96960	.NET のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70162	.NET のサービス拒否の脆弱性	重要	5.9	なし	なし	サービス拒否
CVE-2026-96225	.NET の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96231	.NET の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70161	.NET の特権の昇格の脆弱性	重要	7.3	なし	なし	特権昇格
CVE-2026-70190	.NET の特権の昇格の脆弱性	重要	7.3	なし	なし	特権昇格
CVE-2026-70165	.NET の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-85363	.NET Framework の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-70007	.NET Framework のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70035	.NET Framework のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70194	.NET Framework のセキュリティ機能のバイパスの脆弱性	重要	6.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-97801	.NET Framework の改ざんの脆弱性	重要	7.5	なし	なし	改ざん
CVE-2026-96232	.NET の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-96229	.NET の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-66822	.NET の情報漏洩の脆弱性	重要	5.9	なし	なし	情報漏洩
CVE-2026-96234	.NET の情報漏洩の脆弱性	重要	5.3	なし	なし	情報漏洩
CVE-2026-70174	.NET のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83520	.NET のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-87697	.NET のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-96224	.NET のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-96235	.NET のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70197	.NET のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-96237	.NET のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-96957	.NET のセキュリティ機能のバイパスの脆弱性	重要	8.8	なし	なし	セキュリティ機能のバイパス
CVE-2026-96238	.NET のセキュリティ機能のバイパスの脆弱性	重要	6.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-83666	Active Directory Certificate Services (AD CS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83645	Active Directory Federation Services (AD FS) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-85319	Active Directory Federation Services (AD FS) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-85321	Active Directory Federation Services (AD FS) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-85324	Active Directory Federation Services (AD FS) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-97788	Active Directory Federation Services (AD FS) の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-69982	Active Directory Federation Services (AD FS) 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	セキュリティ機能のバイパス
CVE-2026-70005	Active Directory Federation Services (AD FS) 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	セキュリティ機能のバイパス
CVE-2026-96252	Active Directory Federation Services (AD FS) のなりすましの脆弱性	重要	9.1	なし	なし	なりすまし
CVE-2026-83674	Active Directory Federation Services (AD FS) のなりすましの脆弱性	重要	8.1	なし	なし	なりすまし
CVE-2026-83511	Active Directory Federation Services (AD FS) のなりすましの脆弱性	重要	7.4	なし	なし	なりすまし
CVE-2026-103576	Active Directory Federation Services (AD FS) のなりすましの脆弱性	重要	6.5	なし	なし	なりすまし
CVE-2026-83646	Active Directory Federation Services (AD FS) のなりすましの脆弱性	重要	4.8	なし	なし	なりすまし
CVE-2026-70159	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70181	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70186	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-96233	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-96236	ASP.NET Core のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70196	ASP.NET Core のサービス拒否の脆弱性	重要	5.9	なし	なし	サービス拒否
CVE-2026-70175	ASP.NET Core の特権の昇格の脆弱性	重要	8.1	なし	なし	特権昇格
CVE-2026-70179	ASP.NET Core の特権の昇格の脆弱性	重要	7.5	なし	なし	特権昇格
CVE-2026-70183	ASP.NET Core の特権の昇格の脆弱性	重要	7.5	なし	なし	特権昇格
CVE-2026-102870	ASP.NET Core のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-96230	ASP.NET Core のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70188	ASP.NET Core 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	セキュリティ機能のバイパス
CVE-2026-88092	ASP.NET Core の改ざんの脆弱性	重要	9.4	なし	なし	改ざん
CVE-2026-85916	Azure Active Directory の情報漏洩の脆弱性	重要	6.2	なし	なし	情報漏洩
CVE-2026-96204	Azure Arc の特権の昇格の脆弱性	重要	6.5	なし	なし	特権昇格
CVE-2026-100207	Azure CycleCloud のリモートでコードが実行される脆弱性	重要	7.3	なし	なし	リモートコード実行
CVE-2026-69877	Azure DevOps の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-85891	Azure HDInsight の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-85925	Azure Key Vault Client SDK の特権の昇格の脆弱性	重要	8.2	なし	なし	特権昇格
CVE-2026-88132	Azure Key Vault の情報漏洩の脆弱性	重要	5.9	なし	なし	情報漏洩
CVE-2026-85922	Azure Key Vault のセキュリティ機能のバイパスの脆弱性	重要	7.4	なし	なし	セキュリティ機能のバイパス
CVE-2026-88094	Azure Storage Library の特権の昇格の脆弱性	重要	8.1	なし	なし	特権昇格
CVE-2026-85861	Clipboard User Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85863	Clipboard User Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85912	Clipboard User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88075	Configuration Manager の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-83846	Connected Devices Platform Service (Cdpsvc) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-95943	Connected Devices Platform Service (Cdpsvc) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69880	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69926	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70228	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70255	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88093	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96108	Desktop Window Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70234	Desktop Window Manager の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69974	Desktop Window Manager の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-102226	Dynamics Business Central の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-105728	Dynamics Business Central の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-100214	Dynamics Business Central のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83670	Function Discovery Service (fdwsd.dll) の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-69326	Graphic Fonts のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-105003	HID Class Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-97804	HID Class Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-105006	HID Class Driver の特権の昇格の脆弱性	重要	6.4	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83569	HID Parser Library の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70128	HID Parser Library の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83887	HID Parser Library の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83898	HID Parser Library の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83904	HID Parser Library の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70208	HTTP.sys の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83705	HTTP.sys の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83714	HTTP.sys の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70247	HTTP.sys のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-85856	Internet Connection Sharing (ICS) のリモートでコードが実行される脆弱性	重要	7.1	なし	なし	リモートコード実行
CVE-2026-83741	Internet Explorer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69963	Kernel Streaming Service Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69966	Kernel Streaming Service Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69964	Kernel Streaming Service Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69970	Kernel Streaming Service Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83847	Microsoft Account の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85329	Microsoft Account の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69454	Microsoft Azure Attestation service and Device Health Attestation Service の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-69577	Microsoft Azure Attestation service and Device Health Attestation Service の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-96844	Microsoft Bluetooth Driver の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-83868	Microsoft Bluetooth Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83760	Microsoft Bluetooth Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69909	Microsoft COM for Windows の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-105726	Microsoft Defender の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70264	Microsoft Defender の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-88158	Microsoft Digest Authentication の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-105727	Microsoft Dynamics 365 Business Central の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-77910	Microsoft Exchange Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-96940	Microsoft Exchange Server の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-87692	Microsoft Exchange Server の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-87695	Microsoft Exchange Server の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-87696	Microsoft Exchange Server の特権の昇格の脆弱性	重要	7.5	なし	なし	特権昇格
CVE-2026-70279	Microsoft Exchange Server のなりすましの脆弱性	重要	9.3	なし	なし	なりすまし
CVE-2026-88102	Microsoft Failover Cluster のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-96864	Microsoft Failover Cluster Virtual Driver のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-70123	Microsoft Graphics Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85338	Microsoft Graphics Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102209	Microsoft Graphics Component の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88101	Microsoft Input Method Editor (IME) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-78459	Microsoft Internet Information Services の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83778	Microsoft Internet Messaging API のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83919	Microsoft Internet Messaging API のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-70049	Microsoft Intune の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-83722	Microsoft Local Security Authority (LSA) Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-87710	Microsoft Local Security Authority (LSA) Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-102204	Microsoft Microsoft Defender for Endpoint の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70343	Microsoft MPEG-2 Video Extension のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-94506	Microsoft Office Access の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-102849	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-102850	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-105591	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-105593	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-105595	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-105596	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-105597	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-105598	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-105716	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-105717	Microsoft Office Access のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-105592	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	リモートコード実行
CVE-2026-105714	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	リモートコード実行
CVE-2026-88109	Microsoft Office Click-To-Run の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-97774	Microsoft Office Click-to-Run の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85340	Microsoft Office Click-to-Run の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70276	Microsoft Office Click-to-Run の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69922	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70219	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88151	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88153	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88154	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88172	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88175	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88184	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88190	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88192	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88195	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88201	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97740	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-97743	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97760	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97779	Microsoft Office Excel の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70214	Microsoft Office Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-97014	Microsoft Office Excel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-100212	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70254	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-77902	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88145	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97003	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97004	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97007	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97008	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97010	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97011	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97017	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97738	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97746	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97747	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97748	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97750	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97751	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97752	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97754	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97757	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97762	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-97763	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97766	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97768	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97769	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97770	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97771	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97772	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97773	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97775	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97777	Microsoft Office Excel のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97009	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	リモートコード実行
CVE-2026-105731	Microsoft Office Graphics Component の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85881	Microsoft Office Graphics の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-96997	Microsoft Office OneNote の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102858	Microsoft Office OneNote のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97781	Microsoft Office OneNote のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70281	Microsoft Office Outlook の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-70256	Microsoft Office Outlook のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70257	Microsoft Office Outlook のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70282	Microsoft Office Outlook のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97012	Microsoft Office Outlook のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88183	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88203	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97005	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-97744	Microsoft Office PowerPoint の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-105599	Microsoft Office 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-88196	Microsoft Office のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88197	Microsoft Office のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-102860	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-102861	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-102862	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-102863	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-70246	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-70266	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-88198	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-88200	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-96044	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-70202	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	7.5	なし	なし	特権昇格
CVE-2026-70251	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	7.5	なし	なし	特権昇格
CVE-2026-88206	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	7.5	なし	なし	特権昇格
CVE-2026-105720	Microsoft Office SharePoint の特権の昇格の脆弱性	重要	4.3	なし	なし	特権昇格
CVE-2026-102865	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70259	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70298	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-85932	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70217	Microsoft Office SharePoint の情報漏洩の脆弱性	重要	4.9	なし	なし	情報漏洩
CVE-2026-69943	Microsoft Office SharePoint のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-85900	Microsoft Office SharePoint のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88155	Microsoft Office SharePoint のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88166	Microsoft Office SharePoint のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-105013	Microsoft Office SharePoint のリモートでコードが実行される脆弱性	重要	7.4	なし	なし	リモートコード実行
CVE-2026-70267	Microsoft Office SharePoint 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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-88163	Microsoft Office SharePoint のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97783	Microsoft Office SharePoint のなりすましの脆弱性	重要	8.1	なし	なし	なりすまし
CVE-2026-88204	Microsoft Office SharePoint のなりすましの脆弱性	重要	7.3	なし	なし	なりすまし
CVE-2026-105713	Microsoft Office SharePoint のなりすましの脆弱性	重要	5.7	なし	なし	なりすまし
CVE-2026-102859	Microsoft Office SharePoint のなりすましの脆弱性	重要	4.6	なし	なし	なりすまし
CVE-2026-102864	Microsoft Office SharePoint のなりすましの脆弱性	重要	4.6	なし	なし	なりすまし
CVE-2026-88208	Microsoft Office SharePoint のなりすましの脆弱性	重要	4.6	なし	なし	なりすまし
CVE-2026-88209	Microsoft Office SharePoint のなりすましの脆弱性	重要	4.6	なし	なし	なりすまし
CVE-2026-97782	Microsoft Office SharePoint の改ざんの脆弱性	重要	6.8	なし	なし	改ざん
CVE-2026-96995	Microsoft Office Word の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70206	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70263	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88167	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-88169	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-102867	Microsoft Office Word の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70268	Microsoft Office Word のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70287	Microsoft Office Word のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70301	Microsoft Office Word のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70302	Microsoft Office Word のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83891	Microsoft Office Word のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88150	Microsoft Office Word のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88186	Microsoft Office Word のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88202	Microsoft Office Word のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70220	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	リモートコード実行
CVE-2026-96996	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	リモートコード実行
CVE-2026-97001	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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-105715	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	リモートコード実行
CVE-2026-88210	Microsoft Office Word のセキュリティ機能のバイパスの脆弱性	重要	7.8	なし	なし	セキュリティ機能のバイパス
CVE-2026-70163	Microsoft OpenSSH for Windows のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-83769	Microsoft OpenSSH for Windows の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83871	Microsoft OpenSSH for Windows の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-97811	Microsoft OpenSSH for Windows の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83923	Microsoft OpenSSH for Windows のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88157	Microsoft OpenSSH for Windows のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83754	Microsoft OpenSSH for Windows のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-97816	Microsoft OpenSSH for Windows のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-70092	Microsoft PostScript Printer Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70110	Microsoft PostScript Printer Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70109	Microsoft PostScript Printer Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70213	Microsoft Power Apps のリモートでコードが実行される脆弱性	重要	8	なし	なし	リモートコード実行
CVE-2026-83578	Microsoft PowerShell のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-85817	Microsoft PowerShell のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-96251	Microsoft PowerShell のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70052	Microsoft 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	リモートコード実行
CVE-2026-70185	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	セキュリティ機能のバイパス
CVE-2026-85805	Microsoft PowerShell のセキュリティ機能のバイパスの脆弱性	重要	6.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-96303	Microsoft PowerShell のセキュリティ機能のバイパスの脆弱性	重要	6.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-96188	Microsoft PowerToys の特権の昇格の脆弱性	重要	7.3	なし	なし	特権昇格
CVE-2026-83681	Microsoft PowerToys の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-85790	Microsoft QUIC の情報漏洩の脆弱性	重要	5.9	なし	なし	情報漏洩
CVE-2026-103577	Microsoft QUIC のセキュリティ機能のバイパスの脆弱性	重要	7.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-88193	Microsoft Scripting Engine の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-105719	Microsoft SharePoint Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-67626	Microsoft SQL Server のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-88084	Microsoft SQL Server のサービス拒否の脆弱性	重要	5.3	なし	なし	サービス拒否
CVE-2026-94520	Microsoft SQL Server のサービス拒否の脆弱性	重要	4.9	なし	なし	サービス拒否
CVE-2026-68883	Microsoft SQL Server の特権の昇格の脆弱性	重要	8.5	なし	なし	特権昇格
CVE-2026-85876	Microsoft SQL Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85919	Microsoft SQL Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88082	Microsoft SQL Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88088	Microsoft SQL Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88085	Microsoft SQL Server の特権の昇格の脆弱性	重要	6.4	なし	なし	特権昇格
CVE-2026-85888	Microsoft SQL Server の情報漏洩の脆弱性	重要	7.7	なし	なし	情報漏洩
CVE-2026-88081	Microsoft SQL Server の情報漏洩の脆弱性	重要	7.7	なし	なし	情報漏洩
CVE-2026-88086	Microsoft SQL Server の情報漏洩の脆弱性	重要	5.3	なし	なし	情報漏洩
CVE-2026-67628	Microsoft SQL Server の情報漏洩の脆弱性	重要	4.9	なし	なし	情報漏洩
CVE-2026-65674	Microsoft SQL Server のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-67625	Microsoft SQL Server のリモートでコードが実行される脆弱性	重要	8.5	なし	なし	リモートコード実行
CVE-2026-85886	Microsoft SQL Server のリモートでコードが実行される脆弱性	重要	8.5	なし	なし	リモートコード実行
CVE-2026-88083	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	リモートコード実行
CVE-2026-70189	Microsoft SQL Server のリモートでコードが実行される脆弱性	重要	6.7	なし	なし	リモートコード実行
CVE-2026-88089	Microsoft SQL Server のリモートでコードが実行される脆弱性	重要	6.7	なし	なし	リモートコード実行
CVE-2026-83945	Microsoft SQL Server 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	リモートコード実行
CVE-2026-70260	Microsoft Trace Data Helper の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70261	Microsoft Trace Data Helper の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-102199	Microsoft Windows Codecs Library のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-102201	Microsoft Windows Media Foundation の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70131	Microsoft Windows Media Foundation の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70278	Microsoft Windows Media Foundation の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96186	Microsoft Windows Media Foundation の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70044	Microsoft Windows Media Foundation の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83517	Microsoft Windows Media Foundation のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-85814	Microsoft Windows Media Foundation のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-70258	Microsoft Windows Media Foundation のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-87712	Microsoft Windows QoS Scheduler Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-105010	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	9.8	なし	なし	特権昇格
CVE-2026-70177	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83704	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83829	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83850	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85869	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88182	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88191	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96324	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96911	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70086	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70115	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70136	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70150	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70156	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88160	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96937	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-108136	Microsoft Windows Search Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70141	Microsoft Windows Search Component の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70173	Microsoft Windows Search Component の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83686	Microsoft Windows Search Component の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96910	Microsoft Windows Search Component の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83725	Microsoft Windows Search Component のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-69978	Microsoft Windows VMSwitch のサービス拒否の脆弱性	重要	5.6	なし	なし	サービス拒否
CVE-2026-83935	Microsoft XML のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83914	Microsoft XML のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-96861	Network Device Enrollment Service (NDES) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-96866	Network Device Enrollment Service (NDES) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-85323	Network Device Enrollment Service (NDES) のなりすましの脆弱性	重要	6.8	なし	なし	なりすまし
CVE-2026-83655	Network Policy Server (NPS) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-96246	Network Policy Server (NPS) の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-100222	Network Policy Server (NPS) のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-85806	Network Policy Server (NPS) のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-85371	Network Policy Server (NPS) のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-85799	Network Policy Server (NPS) のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-70207	Network Policy Server (NPS) のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-85811	Network Policy Server (NPS) のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-85864	Python の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69977	Quality Windows Audio/Video Experience (QWAVE) service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85943	Reliable Multicast Transport Driver (RMCAST) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-84015	Remote Access Point-to-Point Protocol (PPP) EAP-TLS のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-103575	Remote Desktop Client のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83688	Remote Desktop Client のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-69976	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	リモートコード実行
CVE-2026-69984	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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69986	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	リモートコード実行
CVE-2026-69987	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	リモートコード実行
CVE-2026-69988	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	リモートコード実行
CVE-2026-69991	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	リモートコード実行
CVE-2026-69994	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	リモートコード実行
CVE-2026-69995	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	リモートコード実行
CVE-2026-69996	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	リモートコード実行
CVE-2026-69997	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	リモートコード実行
CVE-2026-69998	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	リモートコード実行
CVE-2026-70004	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	リモートコード実行
CVE-2026-70006	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	リモートコード実行
CVE-2026-70012	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	リモートコード実行
CVE-2026-97789	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	リモートコード実行
CVE-2026-108458	Remote Desktop Client のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-96321	Remote Desktop Display Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-84007	Remote Desktop Gateway Service の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-100218	Remote Desktop Gateway 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	リモートコード実行
CVE-2026-69992	Remote Desktop Services のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-83635	Role: DNS Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-88122	Role: DNS Server のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-88123	Role: DNS Server のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-88125	Role: DNS Server のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-88129	Role: DNS Server のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-88130	Role: DNS Server のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-108127	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-108128	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-108129	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97817	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97819	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97820	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97821	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97822	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97823	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97824	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97825	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97826	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97827	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97828	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97829	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97831	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97832	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97833	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97834	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97835	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97836	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97837	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97838	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97839	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97840	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97841	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97842	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97843	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-97844	Role: DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70087	Role: DNS Server のセキュリティ機能のバイパスの脆弱性	重要	5.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-103560	Role: DNS Server の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-70071	Role: DNS Server の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-70083	Role: DNS Server の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-70085	Role: DNS Server の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-96926	Role: DNS Server の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-96300	RPC Endpoint Mapper Service のサービス拒否の脆弱性	重要	5.9	なし	なし	サービス拒否
CVE-2026-83518	RPC Runtime の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83908	RPC Runtime の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83515	RPC Runtime の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-83910	RPC Runtime Library のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-88219	RPC Runtime Library のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-102203	RPC Runtime のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83506	Servicing Stack Updates の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83863	Servicing Stack Updates の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85318	Servicing Stack Updates の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85365	Servicing Stack Updates の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96939	Servicing Stack Updates の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83719	Servicing Stack Updates の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85835	Servicing Stack Updates の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83746	Skype for Business の特権の昇格の脆弱性	重要	8.1	なし	なし	特権昇格
CVE-2026-85873	Skype for Business の特権の昇格の脆弱性	重要	6.5	なし	なし	特権昇格
CVE-2026-70297	Skype for Business のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-108464	Software Protection Platform (SPP) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96956	SQL Server の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-94512	SQL Server のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-69867	SQLite の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-105732	SysInternals の特権の昇格の脆弱性	重要	7.3	なし	なし	特権昇格
CVE-2026-100205	SysInternals の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-105729	SysInternals の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-49785	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	なし	なし	セキュリティ機能のバイパス
CVE-2026-70252	Virtual Hard Disk (VHD) Miniport Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-103555	Virtual Hard Disk (VHD) Miniport Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-109453	Virtual Hard Disk (VHD) Miniport Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-102229	Visual Studio Code の情報漏洩の脆弱性	重要	6.8	なし	なし	情報漏洩
CVE-2026-102238	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	リモートコード実行
CVE-2026-102235	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	リモートコード実行
CVE-2026-69370	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	リモートコード実行
CVE-2026-70098	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	リモートコード実行
CVE-2026-102233	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	7.8	なし	なし	セキュリティ機能のバイパス
CVE-2026-102231	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	7.7	なし	なし	セキュリティ機能のバイパス
CVE-2026-102234	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	7.4	なし	なし	セキュリティ機能のバイパス
CVE-2026-102232	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	7	なし	なし	セキュリティ機能のバイパス
CVE-2026-102851	Visual Studio Code のセキュリティ機能のバイパスの脆弱性	重要	6.1	なし	なし	セキュリティ機能のバイパス
CVE-2026-103572	Visual Studio Tools for Applications and SQL Server Management Studio のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-85846	Web Account Manager の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88136	Web Distributed Authoring and Versioning (WEBDAV) のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-102217	WebDAV の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-70262	WebDAV の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-88126	WebDAV の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-88135	WebDAV の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96843	WebDAV の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96847	WebDAV の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85370	WebDAV の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85827	WebDAV の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85828	WebDAV の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88137	WebDAV の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-96846	WebDAV の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-87714	WebDAV のセキュリティ機能のバイパスの脆弱性	重要	6.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-83721	Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83732	Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83757	Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83762	Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83755	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70211	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70284	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70288	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70292	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70293	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70294	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70295	Win32k の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96113	Windows Domain Name Service のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83869	Windows Domain Name Service のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-70167	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	リモートコード実行
CVE-2026-83642	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	リモートコード実行
CVE-2026-85903	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	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-88112	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	リモートコード実行
CVE-2026-88114	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	リモートコード実行
CVE-2026-88116	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	リモートコード実行
CVE-2026-70127	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	リモートコード実行
CVE-2026-83647	Windows Active Directory Domain Services のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-83648	Windows Active Directory Domain Services のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-83667	Windows Active Directory Domain Services のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-88165	Windows Active Directory Domain Services のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-84019	Windows Advanced Rasterization Platform の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83870	Windows Aggregated Data Platform Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69923	Windows AI の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85866	Windows ALPC の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-70225	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70245	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70168	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70205	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70237	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83738	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88149	Windows Ancillary Function Driver for WinSock の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70195	Windows Ancillary Function Driver for WinSock の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-72955	Windows Application Compatibility Cache の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69945	Windows AppX Deployment Extensions の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-85849	Windows AppX Deployment Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85934	Windows AppX Deployment Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69914	Windows AppX Deployment Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69969	Windows AppX Deployment Service の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69979	Windows AppX Deployment Service のセキュリティ機能のバイパスの脆弱性	重要	5.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-69905	Windows AppX Deployment Service の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-96220	Windows Assigned Access の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-97799	Windows Audio Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70118	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70140	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70230	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83644	Windows Audio Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83571	Windows Audio Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96314	Windows Audio Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-108134	Windows Autopilot の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96215	Windows Autopilot の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85832	Windows Background Intelligent Transfer Service (BITS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85843	Windows Background Intelligent Transfer Service (BITS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85848	Windows Background Intelligent Transfer Service (BITS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88118	Windows Background Intelligent Transfer Service (BITS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88152	Windows Background Intelligent Transfer Service (BITS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88146	Windows Background Intelligent Transfer Service (BITS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88142	Windows Background Intelligent Transfer Service (BITS) のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88159	Windows Background Intelligent Transfer Service (BITS) のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88173	Windows Background Intelligent Transfer Service (BITS) のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-88121	Windows Background Intelligent Transfer Service (BITS) のリモートでコードが実行される脆弱性	重要	8	なし	なし	リモートコード実行
CVE-2026-70184	Windows Backup Engine の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-108135	Windows Backup Engine の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-62687	Windows Backup Engine の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70299	Windows Bind Filter Driver の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-70274	Windows Bind Filter Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83692	Windows Bind Filter Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88168	Windows Bind Filter Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83852	Windows Bind Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83900	Windows Bind Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85812	Windows Bind Filter Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85831	Windows Biometric Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83634	Windows BitLocker の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88070	Windows BitLocker の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85920	Windows BitLocker の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96909	Windows BitLocker のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83500	Windows BitLocker のセキュリティ機能のバイパスの脆弱性	重要	6.1	なし	なし	セキュリティ機能のバイパス
CVE-2026-83838	Windows Bluetooth A2DP driver の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-83776	Windows Bluetooth Driver の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-83827	Windows Bluetooth Port Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-87713	Windows Bluetooth Port Driver 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	特権昇格
CVE-2026-70126	Windows Bluetooth Port Driver のリモートでコードが実行される脆弱性	重要	7.1	なし	なし	リモートコード実行
CVE-2026-83777	Windows Bluetooth Service の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-83739	Windows Bluetooth Service のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-102196	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88105	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-97809	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102193	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-102195	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-102197	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-103554	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-103565	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-105722	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88103	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88113	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96919	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-97808	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70122	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	6.5	なし	なし	特権昇格
CVE-2026-97806	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-97807	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-108461	Windows Broadcast DVR User Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70148	Windows Broadcast DVR User Service の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-103567	Windows Broadcast DVR User Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85938	Windows Broadcast DVR User Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83771	Windows Camera Frame Server Monitor の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-83753	Windows Camera Frame Server Monitor の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85803	Windows Camera Frame Server Monitor の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85367	Windows Cash Drawer Protocol Provider の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83780	Windows CCFFilter Driver のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-85377	Windows CD-ROM Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83888	Windows CD-ROM Driver の特権の昇格の脆弱性	重要	6.5	なし	なし	特権昇格
CVE-2026-70041	Windows CD-ROM Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70275	Windows CD-ROM File System Driver のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-69850	Windows Certificates の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69840	Windows Certificates の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69949	Windows Client for NFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70113	Windows Client for NFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69940	Windows Client for NFS の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-69955	Windows Client for NFS の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-96912	Windows Client License Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-100201	Windows Client License Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70149	Windows Client Side Caching driver (csc.sys) の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-96948	Windows Client Side Caching driver (csc.sys) の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70068	Windows Client-Side Caching (CSC) Service の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-83698	Windows Client-Side Caching (CSC) Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83699	Windows Client-Side Caching (CSC) Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83580	Windows Client-Side Caching (CSC) Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69795	Windows Clipboard Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83764	Windows Clipboard User Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83893	Windows Clipboard User Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83696	Windows Cloud Files Mini Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88106	Windows Cloud Files Mini Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88107	Windows Cloud Files Mini Filter Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83830	Windows COM+ Event System Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83848	Windows COM+ Event System Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96933	Windows COM+ Event System Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83785	Windows COM+ Event System Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70233	Windows Common Log File System Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85355	Windows Common Log File System Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85868	Windows Common Log File System Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85870	Windows Common Log File System Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83835	Windows Common Log File System Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85823	Windows Composite Image File System の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85824	Windows Composite Image File System の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70169	Windows Connected Devices Platform Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83687	Windows Connected User Experiences and Telemetry の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70223	Windows Console Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-102202	Windows Container Isolation FS Filter Driver (unionfs.sys) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-97792	Windows Container Isolation FS Filter Driver (unionfs.sys) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-97794	Windows Container Isolation FS Filter Driver (unionfs.sys) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-97787	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	特権昇格
CVE-2026-97810	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	特権昇格
CVE-2026-97790	Windows Container Isolation FS Filter Driver (unionfs.sys) の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-70270	Windows Container Isolation FS Filter Driver の特権の昇格の脆弱性	重要	5.5	なし	なし	特権昇格
CVE-2026-69918	Windows Core Messaging の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-83587	Windows Core Messaging の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70580	Windows Credential Guard のなりすましの脆弱性	重要	8.8	なし	なし	なりすまし
CVE-2026-69736	Windows Credential Manager の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-103568	Windows Credential Providers の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69919	Windows Cryptographic Services の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70055	Windows Cryptographic Services の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70014	Windows Cryptographic Services のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-88096	Windows DCOM Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83679	Windows Defender Firewall Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85332	Windows Device Association Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83710	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-84014	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-85342	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85352	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85904	Windows Device Association Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85331	Windows Device Association Service の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70227	Windows Device Association Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85336	Windows Device Association Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85815	Windows Device Association Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96854	Windows Device Association Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83792	Windows Device Install Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83877	Windows Devices Human Interface の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83677	Windows DHCP Client のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-83665	Windows DHCP Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70201	Windows DHCP Server のサービス拒否の脆弱性	重要	5.5	なし	なし	サービス拒否
CVE-2026-83691	Windows DHCP Server の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70066	Windows DHCP Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96320	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	リモートコード実行
CVE-2026-70069	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-69830	Windows DHCP Server のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-70058	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	リモートコード実行
CVE-2026-85841	Windows DHCP Server 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	リモートコード実行
CVE-2026-83787	Windows DHCP Server のセキュリティ機能のバイパスの脆弱性	重要	5.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-85865	Windows DHCP Server のセキュリティ機能のバイパスの脆弱性	重要	5.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-83915	Windows Diagnostic Policy Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83896	Windows Direct Composition の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83902	Windows Direct Composition の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83903	Windows Direct Composition の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83912	Windows Direct Composition の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83922	Windows Direct Composition の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85902	Windows Direct Composition の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85906	Windows Direct Composition の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70151	Windows Direct Composition の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70021	Windows Direct Composition の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-105723	Windows Distributed File System (DFS) の特権の昇格の脆弱性	重要	7.5	なし	なし	特権昇格
CVE-2026-96938	Windows Distributed File System (DFS) の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-85931	Windows Distributed File System (DFS) のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-85798	Windows Distributed File System (DFS) 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	リモートコード実行
CVE-2026-70082	Windows DNS のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70079	Windows DNS のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70155	Windows DNS のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70166	Windows DNS のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-70074	Windows DNS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70119	Windows DNS 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	リモートコード実行
CVE-2026-70244	Windows DNS Server の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-83889	Windows DNS Server のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83726	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88128	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88177	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88179	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88180	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88181	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88188	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88189	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-88194	Windows DWM Core Library の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85853	Windows DWM Core Library の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85854	Windows DWM Core Library の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85855	Windows DWM Core Library の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83765	Windows DWM Core Library の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-84016	Windows EAPHost Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85914	Windows Embedded Mode Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96932	Windows Embedded Mode Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83784	Windows Encrypting File System (EFS) の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-85791	Windows Encrypting File System (EFS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83683	Windows Encrypting File System (EFS) の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-83565	Windows Encrypting File System (EFS) の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83759	Windows Encrypting File System (EFS) のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-88162	Windows Encrypting File System (EFS) の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-69452	Windows Enterprise App Management の特権の昇格の脆弱性	重要	7.1	なし	なし	特権昇格
CVE-2026-69354	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69363	Windows Error Reporting の特権の昇格の脆弱性	重要	8	なし	なし	特権昇格
CVE-2026-70103	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83669	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83826	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83840	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85800	Windows Error Reporting の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69387	Windows Error Reporting の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83689	Windows Error Reporting の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83750	Windows Error Reporting の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85354	Windows Error Reporting の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83658	Windows Error Reporting の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83747	Windows Error Reporting の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83519	Windows Error Reporting のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83693	Windows Error Reporting のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83748	Windows Error Reporting のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-97815	Windows Error Reporting のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83643	Windows Error Reporting のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83758	Windows Error Reporting のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-83916	Windows Error Reporting のリモートでコードが実行される脆弱性	重要	7	なし	なし	リモートコード実行
CVE-2026-97798	Windows Error Reporting Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83715	Windows Error Reporting の改ざんの脆弱性	重要	7.1	なし	なし	改ざん
CVE-2026-83695	Windows Event Logging Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83723	Windows Event Logging Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-95904	Windows Event Logging Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83856	Windows Event Logging Service のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-70134	Windows Event Tracing の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83707	Windows Event Tracing の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83874	Windows Event Tracing のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83836	Windows Event Tracing のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-70235	Windows Event Tracing のなりすましの脆弱性	重要	5.5	なし	なし	なりすまし
CVE-2026-85840	Windows Event Viewer の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-83881	Windows exFAT File System の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85822	Windows exFAT File System の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102192	Windows Failover Cluster のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-96945	Windows Failover Cluster のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-88099	Windows Failover Cluster のサービス拒否の脆弱性	重要	5.9	なし	なし	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-85826	Windows Fast FAT Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70277	Windows Fast FAT File System Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-87707	Windows Fax and Scan Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83860	Windows GDI のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69884	Windows GDI の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83651	Windows GDI の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-85797	Windows GDI の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70089	Windows GDI のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83929	Windows GDI のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83583	Windows Geotag Broker の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70286	Windows Graphics Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85901	Windows Graphics Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85908	Windows Graphics Component の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96118	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102194	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88110	Windows Graphics Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83582	Windows Graphics Kernel の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-100217	Windows Group Policy の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83932	Windows Group Policy の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85884	Windows Health and Optimized Experiences Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96183	Windows Health and Optimized Experiences Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83740	Windows Hello の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83790	Windows Hello の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83853	Windows Hello の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83849	Windows Hello の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83907	Windows Hello の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70280	Windows Hello のセキュリティ機能のバイパスの脆弱性	重要	4.4	なし	なし	セキュリティ機能のバイパス
CVE-2026-83926	Windows Hello のセキュリティ機能のバイパスの脆弱性	重要	4.4	なし	なし	セキュリティ機能のバイパス
CVE-2026-96248	Windows Host Guardian Service のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-88072	Windows Host Guardian Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-87709	Windows Host Guardian Service の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-83875	Windows Human Interface Device の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83884	Windows Human Interface Device の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83892	Windows Human Interface Device の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70248	Windows Hyper-V のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-83636	Windows Hyper-V のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-85369	Windows Hyper-V の特権の昇格の脆弱性	重要	8.2	なし	なし	特権昇格
CVE-2026-70023	Windows Hyper-V の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85343	Windows Hyper-V の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88071	Windows Hyper-V の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96223	Windows Hyper-V の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83839	Windows Hyper-V の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83671	Windows Hyper-V の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-97813	Windows Hyper-V の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-83716	Windows Hyper-V のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83931	Windows Hyper-V のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-87705	Windows Hyper-V のセキュリティ機能のバイパスの脆弱性	重要	7.4	なし	なし	セキュリティ機能のバイパス
CVE-2026-83766	Windows Hyper-V のセキュリティ機能のバイパスの脆弱性	重要	4.2	なし	なし	セキュリティ機能のバイパス
CVE-2026-83728	Windows Hyper-V のなりすましの脆弱性	重要	8.8	なし	なし	なりすまし
CVE-2026-103569	Windows IKE Extension の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-83521	Windows IKE Extension の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-83522	Windows IKE Extension のなりすましの脆弱性	重要	8.1	なし	なし	なりすまし

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-85842	Windows Image Acquisition の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85930	Windows Image Acquisition の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83523	Windows Image Acquisition のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-96859	Windows Imaging Component の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69886	Windows Imaging Component のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-77496	Windows Imaging Component のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83763	Windows Input System の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69471	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83767	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83779	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85358	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85366	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85796	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-87694	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-87700	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-87711	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88080	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96308	Windows Installer の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70272	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83676	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83680	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83702	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83708	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83717	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83718	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83752	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83775	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83899	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85361	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85364	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85941	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-87693	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-87704	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-87708	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-87715	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88076	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88124	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96302	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96305	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96307	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69635	Windows Installer の特権の昇格の脆弱性	重要	6.6	なし	なし	特権昇格
CVE-2026-108468	Windows Installer の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85374	Windows Installer の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85830	Windows Installer の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83672	Windows Installer の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-96244	Windows Internal System User Profile の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83845	Windows Internet (wininet.dll) のなりすましの脆弱性	重要	8.4	なし	なし	なりすまし
CVE-2026-83865	Windows Internet (wininet.dll) の改ざんの脆弱性	重要	4.7	なし	なし	改ざん
CVE-2026-97830	Windows Internet Information Services のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-70024	Windows Internet Information Services のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83795	Windows Internet Key Exchange (IKE) Extension のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-83843	Windows Internet Key Exchange (IKE) Extension のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83685	Windows Internet Key Exchange (IKE) Extension のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-70008	Windows IP Over USB Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70011	Windows IP Over USB Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70031	Windows iSCSI のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-69644	Windows iSCSI の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69721	Windows iSCSI の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69521	Windows iSCSI のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-69634	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	リモートコード実行
CVE-2026-69705	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	リモートコード実行
CVE-2026-69883	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	リモートコード実行
CVE-2026-70013	Windows iSCSI のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-70038	Windows iSCSI のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-70095	Windows iSCSI のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-70064	Windows Kerberos の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70241	Windows Kerberos の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83720	Windows Kerberos の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-108132	Windows Kerberos の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70170	Windows Kernel のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-108466	Windows Kernel のサービス拒否の脆弱性	重要	5.3	なし	なし	サービス拒否
CVE-2026-70111	Windows Kernel の特権の昇格の脆弱性	重要	8.1	なし	なし	特権昇格
CVE-2026-69898	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70106	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70114	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70121	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70303	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83690	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83735	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83768	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83796	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83833	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83882	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83913	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83918	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85836	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85837	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85850	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85945	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88134	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96312	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96317	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96929	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102207	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70160	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70243	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83675	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83924	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85372	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88139	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88141	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96216	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96868	Windows Kernel の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-103578	Windows Kernel の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83736	Windows Kernel の特権の昇格の脆弱性	重要	5.5	なし	なし	特権昇格
CVE-2026-97803	Windows Kernel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102187	Windows Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70199	Windows Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70232	Windows Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70063	Windows Kernel の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-70077	Windows Kernel の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-83925	Windows Kernel の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-108462	Windows Kernel の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85939	Windows Kernel 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	セキュリティ機能のバイパス
CVE-2026-83573	Windows Kernel-Mode Driver の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-83568	Windows Kernel-Mode Drivers の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83637	Windows Kernel-Mode Drivers の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83837	Windows Kernel-Mode Drivers の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85871	Windows Kernel-Mode Drivers の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96915	Windows Kernel-Mode Drivers の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83834	Windows Kernel-Mode Drivers の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69971	Windows Kernel-Mode Drivers の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85857	Windows Kernel-Mode Drivers の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96247	Windows Kernel-Mode Drivers の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96849	Windows Kernel-Mode Drivers の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-68836	Windows kernel32.dll の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69650	Windows Key Distribution Center の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69640	Windows Key Distribution Center 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	セキュリティ機能のバイパス
CVE-2026-88140	Windows Key Storage Provider の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69506	Windows Key Storage Provider の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-69639	Windows libarchive のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-69985	Windows libarchive のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70062	Windows libarchive のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-69968	Windows libarchive の改ざんの脆弱性	重要	6.5	なし	なし	改ざん
CVE-2026-69973	Windows libarchive の改ざんの脆弱性	重要	6.5	なし	なし	改ざん
CVE-2026-88161	Windows Local Security Authority (LSA) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83516	Windows Local Security Authority Subsystem Service (LSASS) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-83649	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	サービス拒否
CVE-2026-70015	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	特権昇格
CVE-2026-96219	Windows Local Security Authority Subsystem Service (LSASS) のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83928	Windows Local Security Authority Subsystem Service (LSASS) のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83783	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88091	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96856	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83724	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85362	Windows Management Instrumentation の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85852	Windows Management Instrumentation の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96851	Windows Management Instrumentation の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-87691	Windows Management Services の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83641	Windows Media の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83650	Windows Media の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96096	Windows Media Player のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-96071	Windows Media のリモートでコードが実行される脆弱性	重要	7.5	なし	なし	リモートコード実行
CVE-2026-85859	Windows Message Queuing Queue Manager のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-85860	Windows Message Queuing Queue Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-85334	Windows Message Queuing Queue Manager の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-96921	Windows Message Queuing Queue Manager の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85874	Windows Message Queuing Queue Manager のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-83828	Windows MIDI Service Module の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83751	Windows MIDI Service Module の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88079	Windows MIDI Service Module の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83773	Windows MIDI Service Module の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-97800	Windows Mobile Broadband の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70216	Windows Mobile Device Management の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-108133	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83654	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85833	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-108396	Windows Modern Device Management (MDM) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96850	Windows Modern Device Management (MDM) の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83657	Windows Modern Device Management (MDM) の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-96855	Windows Modern Device Management (MDM) の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-83656	Windows Modern Device Management (MDM) の改ざんの脆弱性	重要	4.7	なし	なし	改ざん
CVE-2026-83697	Windows Modern Device Management (MDM) の改ざんの脆弱性	重要	4.7	なし	なし	改ざん
CVE-2026-105007	Windows NDIS の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-70054	Windows NetBIOS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70072	Windows Netlogon のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-70025	Windows Netlogon のサービス拒否の脆弱性	重要	5.3	なし	なし	サービス拒否
CVE-2026-70090	Windows Netlogon の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96209	Windows Network File System の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69675	Windows Network File System の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-102186	Windows Network File System の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70143	Windows Network File System のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-96311	Windows Network List Service の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-83862	Windows Network Load Balancing のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83854	Windows Notification の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83700	Windows Now Playing Session Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83701	Windows Now Playing Session Manager の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83706	Windows NTFS の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-69916	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70010	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70172	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83508	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83567	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83585	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83652	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83859	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96217	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96916	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96918	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96928	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96931	Windows NTFS の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69915	Windows NTFS の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-81971	Windows NTFS の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83737	Windows NTFS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83864	Windows NTFS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96925	Windows NTFS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96927	Windows NTFS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-96935	Windows NTFS の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83786	Windows NTFS の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-83640	Windows NTFS のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-83712	Windows NTFS のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-96867	Windows NTFS のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-69902	Windows NTFS のリモートでコードが実行される脆弱性	重要	6.7	なし	なし	リモートコード実行
CVE-2026-83709	Windows NTLM の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70210	Windows OLE DB の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-70059	Windows OLE の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70138	Windows OLE の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96924	Windows OLE のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-105004	Windows Overlay Filter の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69950	Windows Overlay Filter の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69952	Windows Overlay Filter の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69953	Windows Overlay Filter の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69957	Windows Overlay Filter の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83727	Windows Overlay Filter の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83749	Windows Overlay Filter の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83879	Windows Overlay Filter の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69954	Windows Overlay Filter の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69967	Windows Overlay Filter の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-69942	Windows Overlay Filter のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-69959	Windows Overlay Filter のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-69947	Windows Overlay Filter のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	リモートコード実行
CVE-2026-69958	Windows Overlay Filter のリモートでコードが実行される脆弱性	重要	6.8	なし	なし	リモートコード実行
CVE-2026-96315	Windows Overlay Filter の改ざんの脆弱性	重要	5.5	なし	なし	改ざん

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83844	Windows Paint のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-83851	Windows Partition Management Driver の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-103553	Windows Partition Management Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83514	Windows Partition Management Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83797	Windows Partition Management Driver のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-97805	Windows Partition Management Driver のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-96917	Windows PCI Bus Driver の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-85915	Windows PCI Bus Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-61931	Windows Perception Simulation Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85359	Windows Performance Monitor の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85333	Windows Performance Monitor の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-85357	Windows Phone Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-88133	Windows Portable Device Enumerator Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70132	Windows Portable Device File System Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83664	Windows Portable Device File System Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-102206	Windows Portable Device MTP Driver の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-83794	Windows Portable Device MTP Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85327	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85376	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85933	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-84018	Windows Print Spooler Components の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85353	Windows Print Spooler Components の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-85847	Windows Print Spooler Components の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-83733	Windows Print Spooler Components の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85320	Windows Print Spooler Components の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83781	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-96920	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69596	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69743	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-72934	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-72968	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-72969	Windows Program Compatibility Assistant Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85328	Windows Projected File System の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70084	Windows Projected File System の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96857	Windows Projected File System の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-84009	Windows Projected File System の改ざんの脆弱性	重要	4.7	なし	なし	改ざん
CVE-2026-83867	Windows Push Notifications の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70198	Windows Push Notifications の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96313	Windows Push Notifications の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83927	Windows Registry の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85867	Windows Remote Access Connection Manager の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70137	Windows Remote Access Connection Manager の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-87698	Windows Remote Access Service Infrastructure の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85337	Windows Remote Desktop Client の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-70033	Windows Remote Desktop Gateway (RD Gateway) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-83861	Windows Remote Desktop Protocol の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96322	Windows Remote Desktop Protocol の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-102198	Windows Remote Desktop Protocol の情報漏洩の脆弱性	重要	5.3	なし	なし	情報漏洩
CVE-2026-59116	Windows Remote Desktop 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	セキュリティ機能のバイパス
CVE-2026-84012	Windows Remote Desktop Services のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-70135	Windows Remote POS Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83586	Windows Resilient File System (ReFS) Deduplication Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70048	Windows Resilient File System (ReFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102227	Windows Resilient File System (ReFS) のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-70116	Windows Resilient File System (ReFS) のセキュリティ機能のバイパスの脆弱性	重要	4.2	なし	なし	セキュリティ機能のバイパス
CVE-2026-87702	Windows Resource Management (MRM) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96318	Windows Resume の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70093	Windows Rich Text Edit Control の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70096	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	9.8	なし	なし	リモートコード実行
CVE-2026-83788	Windows rndismp6.sys の情報漏洩の脆弱性	重要	4.6	なし	なし	情報漏洩
CVE-2026-103558	Windows Routing and Remote Access Service (RRAS) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-84017	Windows Routing and Remote Access Service (RRAS) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-85808	Windows Routing and Remote Access Service (RRAS) のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-84020	Windows Routing and Remote Access Service (RRAS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85322	Windows Routing and Remote Access Service (RRAS) の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-96245	Windows Routing and Remote Access Service (RRAS) の情報漏洩の脆弱性	重要	7.5	なし	なし	情報漏洩
CVE-2026-85794	Windows Routing and Remote Access Service (RRAS) の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85792	Windows Routing and Remote Access Service (RRAS) のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-85809	Windows Routing and Remote Access Service (RRAS) のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-70158	Windows Routing and Remote Access Service (RRAS) のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-85339	Windows Routing and Remote Access Service (RRAS) のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70057	Windows Routing and Remote Access Service (RRAS) のセキュリティ機能のバイパスの脆弱性	重要	5.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-96316	Windows Routing and Remote Access Service (RRAS) の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-70566	Windows Schannel の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-105005	Windows Schannel のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-105008	Windows Schannel のなりすましの脆弱性	重要	9	なし	なし	なりすまし

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-85818	Windows Schannel のなりすましの脆弱性	重要	9	なし	なし	なりすまし
CVE-2026-83570	Windows Search Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83920	Windows Search Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83564	Windows Search Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83574	Windows Search Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83575	Windows Search Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83921	Windows Search Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-102221	Windows Secure Boot のセキュリティ機能のバイパスの脆弱性	重要	4.4	なし	なし	セキュリティ機能のバイパス
CVE-2026-70026	Windows Secure Kernel Mode の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96865	Windows Secure Kernel Mode の情報漏洩の脆弱性	重要	5.6	なし	なし	情報漏洩
CVE-2026-70017	Windows Secure Kernel Mode の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-88147	Windows Secure Socket Tunneling Protocol (SSTP) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85926	Windows Secure Socket Tunneling Protocol (SSTP) のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-96858	Windows Security Account Manager の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-105725	Windows Security App の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70212	Windows Security Center の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-71347	Windows Security Center の特権の昇格の脆弱性	重要	6.4	なし	なし	特権昇格
CVE-2026-88098	Windows Security Support Provider Interface の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83639	Windows Sensor Data Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88115	Windows Server 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	リモートコード実行
CVE-2026-81969	Windows Server Update Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83499	Windows Server Update Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-105009	Windows Server Update Service の特権の昇格の脆弱性	重要	7.5	なし	なし	特権昇格
CVE-2026-97793	Windows Setup and Deployment の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-73027	Windows Setup Files Cleanup の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83505	Windows Setup Files Cleanup の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83509	Windows Setup Files Cleanup の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83510	Windows Setup Files Cleanup の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70222	Windows Shell の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83873	Windows Shell の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83876	Windows Shell の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83905	Windows Shell の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-83782	Windows Shell のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-85936	Windows Shell のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-83906	Windows Shell のなりすましの脆弱性	重要	6.5	なし	なし	なりすまし
CVE-2026-83579	Windows Smart Card の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83584	Windows Smart Card の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70051	Windows SmartScreen の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85851	Windows SmartScreen の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83504	Windows SmartScreen の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-108463	Windows SmartScreen のセキュリティ機能のバイパスの脆弱性	重要	8.8	なし	なし	セキュリティ機能のバイパス
CVE-2026-62879	Windows SmartScreen の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-83789	Windows SMB Client の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-84011	Windows SMB Client のセキュリティ機能のバイパスの脆弱性	重要	5.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-70133	Windows SMB Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-96325	Windows SMB Server のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-88127	Windows SMB Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69934	Windows Spaceport.sys の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70102	Windows Spaceport.sys の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83832	Windows Spaceport.sys の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96862	Windows Spaceport.sys の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70112	Windows Spaceport.sys のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-102216	Windows StateRepository API の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70218	Windows StateRepository API の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85911	Windows StateRepository API の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85910	Windows StateRepository API の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-100216	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-100225	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-102189	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-102191	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69763	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69766	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69856	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69931	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69935	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83911	Windows Storage の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96944	Windows Storage の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-102188	Windows Storage Port Driver の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-96863	Windows Storage Port Driver の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-88226	Windows Storage Port Driver の情報漏洩の脆弱性	重要	4.6	なし	なし	情報漏洩
CVE-2026-87716	Windows Storage Spaces Controller のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-87706	Windows Storage Spaces Controller の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70238	Windows Storage Spaces Controller の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88100	Windows Storage Spaces Controller の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-88143	Windows Storage Spaces Controller の特権の昇格の脆弱性	重要	6.7	なし	なし	特権昇格
CVE-2026-85872	Windows Storage VSP Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69765	Windows Storport Miniport Driver のリモートでコードが実行される脆弱性	重要	8.8	なし	なし	リモートコード実行
CVE-2026-70027	Windows Subsystem for Linux の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-96309	Windows Subsystem for Linux の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85879	Windows Subsystem for Linux の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96206	Windows Subsystem for Linux の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-96306	Windows Sysmain Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85793	Windows Sysmain Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70157	Windows System Information Console のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83678	Windows TCP/IP の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85368	Windows TCP/IP の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70164	Windows TCP/IP の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83682	Windows TCP/IP の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83842	Windows TCP/IP の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85834	Windows TCP/IP の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96852	Windows TCP/IP の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83872	Windows TCP/IP Local の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69913	Windows TCP/IP のリモートでコードが実行される脆弱性	重要	8.1	なし	なし	リモートコード実行
CVE-2026-84013	Windows Telephony Server の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85810	Windows Telephony Server の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85795	Windows Text Services Framework の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102210	Windows Text Shaping のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-83770	Windows Text Shaping のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-85905	Windows UI Immersive Server API の特権の昇格の脆弱性	重要	8.8	なし	なし	特権昇格
CVE-2026-102205	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102215	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102218	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83513	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83857	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-85820	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96946	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96947	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96950	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85825	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96949	Windows Universal Disk Format File System Driver (UDFS) の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85821	Windows Universal Disk Format File System Driver (UDFS) の情報漏洩の脆弱性	重要	6.5	なし	なし	情報漏洩
CVE-2026-83713	Windows Universal Disk Format File System Driver (UDFS) の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85909	Windows Universal Disk Format File System Driver (UDFS) の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96930	Windows Universal Disk Format File System Driver (UDFS) の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96953	Windows Universal Disk Format File System Driver (UDFS) のリモートでコードが実行される脆弱性	重要	7.8	なし	なし	リモートコード実行
CVE-2026-85373	Windows Universal Plug and Play (UPnP) Device Host の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85375	Windows Universal Plug and Play (UPnP) Device Host の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85927	Windows Universal Plug and Play (UPnP) Device Host の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85918	Windows Universal Plug and Play (UPnP) Device Host の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-108465	Windows Update Delivery Optimization の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69633	Windows Update の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69673	Windows Update の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69718	Windows Update の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69733	Windows Update の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69783	Windows Update の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-69882	Windows Update の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96323	Windows Update の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69999	Windows Update の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83793	Windows Update Orchestrator Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83886	Windows Update Orchestrator Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-83930	Windows Update Orchestrator Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-97812	Windows Update Orchestrator Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83507	Windows Update Orchestrator Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83933	Windows Update Orchestrator Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-81964	Windows Update Orchestrator Service のセキュリティ機能のバイパスの脆弱性	重要	5.5	なし	なし	セキュリティ機能のバイパス
CVE-2026-70139	Windows Update Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70142	Windows Update Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-100200	Windows Update Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-100203	Windows Update Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70056	Windows Update Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83798	Windows Update Stack のなりすましの脆弱性	重要	5.5	なし	なし	なりすまし
CVE-2026-96218	Windows Update Stack の改ざんの脆弱性	重要	5.5	なし	なし	改ざん
CVE-2026-83588	Windows USB Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83638	Windows USB Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85935	Windows USB Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-96250	Windows USB Print Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96253	Windows USB Print Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96254	Windows USB Print Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96301	Windows USB Print Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96304	Windows USB Print Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96310	Windows USB Print Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96319	Windows USB Print Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96860	Windows USB Print Driver の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-85341	Windows USB Video Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85807	Windows USB Video Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83659	Windows User Profile Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-102220	Windows VHD miniport driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83791	Windows Virtual Input の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70075	Windows Virtualization-Based Security (VBS) Enclave のセキュリティ機能のバイパスの脆弱性	重要	4.4	なし	なし	セキュリティ機能のバイパス
CVE-2026-70097	Windows Virtualization-Based Security (VBS) Enclave のなりすましの脆弱性	重要	5.6	なし	なし	なりすまし
CVE-2026-83885	Windows Virtualization-Based Security (VBS) Enclave のなりすましの脆弱性	重要	5.6	なし	なし	なりすまし
CVE-2026-85356	Windows Volume Manager Extension Driver の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83694	Windows Volume Manager Extension Driver の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85928	Windows Volume Manager Extension Driver のリモートでコードが実行される脆弱性	重要	9.8	なし	なし	リモートコード実行
CVE-2026-96243	Windows WalletService の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83703	Windows Wi-Fi Driver のサービス拒否の脆弱性	重要	6.5	なし	なし	サービス拒否
CVE-2026-85816	Windows Wi-Fi Driver の情報漏洩の脆弱性	重要	5.7	なし	なし	情報漏洩
CVE-2026-83756	Windows Win32 Kernel Subsystem の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83761	Windows Win32 Kernel Subsystem の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85804	Windows Win32 Kernel Subsystem の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85858	Windows Win32 Kernel Subsystem の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-96249	Windows Win32 Kernel Subsystem の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-102208	Windows Win32 Kernel Subsystem の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83901	Windows Win32 Kernel Subsystem の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-85802	Windows Win32 Kernel Subsystem の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83895	Windows Win32 Kernel Subsystem の特権の昇格の脆弱性	重要	6.8	なし	なし	特権昇格
CVE-2026-96848	Windows Win32 Kernel Subsystem の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-83774	Windows Win32 Kernel Subsystem の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-83897	Windows Win32 Kernel Subsystem の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-83909	Windows Win32 Kernel Subsystem の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-96853	Windows Win32 Kernel Subsystem の情報漏洩の脆弱性	重要	4.7	なし	なし	情報漏洩
CVE-2026-70067	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格

CVE	脆弱性の名称	深刻度	CVSS	一般公開	悪用	種類
CVE-2026-70060	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70104	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70108	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70117	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70285	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83883	Windows Win32k の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-70076	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70144	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70176	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70209	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70236	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70249	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70253	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70271	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-70273	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83566	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83841	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-83866	Windows Win32k の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-69798	Windows Wired AutoConfig Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-85829	Windows Wired AutoConfig Service の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格
CVE-2026-83855	Windows WLAN Service のサービス拒否の脆弱性	重要	7.5	なし	なし	サービス拒否
CVE-2026-83668	Windows WLAN Service の情報漏洩の脆弱性	重要	5.5	なし	なし	情報漏洩
CVE-2026-70045	Windows Work Folders の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-96923	Windows Workstation Service の特権の昇格の脆弱性	重要	7	なし	なし	特権昇格
CVE-2026-87699	Winlogon の特権の昇格の脆弱性	重要	7.8	なし	なし	特権昇格

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