Microsoft が 2026 年 4 月に公開した CVE の全一覧は以下のとおりです。

CVE	タイトル	深刻度	CVSS	公開	悪用	種類
CVE-2026-32201	Microsoft SharePoint Server のスプーフィングの脆弱性	重要	6.5	No	Yes	なりすまし
CVE-2026-5281 *	Chromium: CVE-2026-5281 Dawn における解放後使用	高	N/A	No	Yes	リモートコード実行
CVE-2026-33825	Microsoft Defender の特権昇格の脆弱性	重要	7.8	Yes	No	特権昇格
CVE-2026-23666	.NET Framework のサービス拒否の脆弱性	緊急	7.5	No	No	DoS攻撃
CVE-2026-32190	Microsoft Office のリモート コード実行の脆弱性	緊急	8.4	No	No	リモートコード実行
CVE-2026-33114	Microsoft Word のリモート コード実行の脆弱性	緊急	8.4	No	No	リモートコード実行
CVE-2026-33115	Microsoft Word のリモート コード実行の脆弱性	緊急	8.4	No	No	リモートコード実行
CVE-2026-32157	リモート デスクトップ クライアントのリモート コード実行の脆弱性	緊急	8.8	No	No	リモートコード実行
CVE-2026-33826	Windows Active Directory のリモート コード実行の脆弱性	緊急	8	No	No	リモートコード実行
CVE-2026-33824	Windows Internet Key Exchange (IKE) Service Extensions のリモート コード実行の脆弱性	緊急	9.8	No	No	リモートコード実行
CVE-2026-33827	Windows TCP/IP のリモート コード実行の脆弱性	緊急	8.1	No	No	リモートコード実行
CVE-2026-26171	.NET のサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
CVE-2026-32226	.NET Framework のサービス拒否の脆弱性	重要	5.9	No	No	DoS攻撃
CVE-2026-32178	.NET のスプーフィングの脆弱性	重要	7.5	No	No	なりすまし
CVE-2026-32203	.NET および Visual Studio のサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
CVE-2026-33116	.NET、.NET Framework、および Visual Studio のサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
CVE-2023-20585 *	AMD: CVE-2023-20585 IOMMU Write Buffer の脆弱性	重要	5.3	No	No	リモートコード実行
CVE-2026-32072	Active Directory のスプーフィングの脆弱性	重要	6.2	No	No	なりすまし
CVE-2026-25184	Applocker Filter Driver (applockerfltr.sys) の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32171	Azure Logic Apps の特権昇格の脆弱性	重要	8.8	No	No	特権昇格
CVE-2026-32168	Azure Monitor Agent の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32192	Azure Monitor Agent の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32181	Connected User Experiences and Telemetry Service のサービス拒否の脆弱性	重要	5.5	No	No	DoS攻撃
CVE-2026-27924	Desktop Window Manager の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32152	Desktop Window Manager の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32154	Desktop Window Manager の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-27923	Desktop Window Manager の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32155	Desktop Window Manager の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-23653	GitHub Copilot および Visual Studio Code の情報漏洩の脆弱性	重要	5.7	No	No	情報漏洩
CVE-2026-23653 *	GitHub: CVE-2026-32631 改ざんされたリポジトリからの 'git clone' により NTLM ハッシュが漏洩する	重要	7.4	No	No	情報漏洩
CVE-2026-33096	HTTP.sys のサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
CVE-2026-25250 *	MITRE: CVE-2026-25250 Eazy Fix による Secure Boot の無効化	重要	6	No	No	セキュリティ機能バイパス
CVE-2026-26181	Microsoft Brokering File System の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32219	Microsoft Brokering File System の特権昇格の脆弱性	重要	7	No	No	特権昇格

CVE-2026-32091	Microsoft Brokering File System の特権昇格の脆弱性	重要	8.4	No	No	特権昇格
CVE-2026-26152	Microsoft Cryptographic Services の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-33103	Microsoft Dynamics 365 (On-Premises) の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-32188	Microsoft Excel の情報漏洩の脆弱性	重要	7.1	No	No	情報漏洩
CVE-2026-32189	Microsoft Excel のリモート コード実行の脆弱性	重要	7.8	No	No	リモートコード実行
CVE-2026-32197	Microsoft Excel のリモート コード実行の脆弱性	重要	7.8	No	No	リモートコード実行
CVE-2026-32198	Microsoft Excel のリモート コード実行の脆弱性	重要	7.8	No	No	リモートコード実行
CVE-2026-32199	Microsoft Excel のリモート コード実行の脆弱性	重要	7.8	No	No	リモートコード実行
CVE-2026-32184	Microsoft 高 Performance Compute (HPC) Pack の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26155	Microsoft Local Security Authority Subsystem Service の情報漏洩の脆弱性	重要	6.5	No	No	情報漏洩
CVE-2026-27914	Microsoft Management Console の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26149	Microsoft Power Apps のセキュリティ機能バイパス	重要	9	No	No	セキュリティ機能バイパス
CVE-2026-32200	Microsoft PowerPoint のリモート コード実行の脆弱性	重要	7.8	No	No	リモートコード実行
CVE-2026-26143	Microsoft PowerShell のセキュリティ機能バイパスの脆弱性	重要	7.8	No	No	セキュリティ機能バイパス
CVE-2026-33120 †	Microsoft SQL Server のリモート コード実行の脆弱性	重要	8.8	No	No	リモートコード実行
CVE-2026-20945	Microsoft SharePoint Server のスプーフィングの脆弱性	重要	4.6	No	No	なりすまし
CVE-2026-33822	Microsoft Word の情報漏洩の脆弱性	重要	6.1	No	No	情報漏洩
CVE-2026-33095	Microsoft Word のリモート コード実行の脆弱性	重要	7.8	No	No	リモートコード実行
CVE-2026-23657	Microsoft Word のリモート コード実行の脆弱性	重要	7.8	No	No	リモートコード実行
CVE-2026-32081	Package Catalog の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-26170	PowerShell の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26183	Remote Access Management service/API (RPC server) の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26160	Remote Desktop Licensing Service の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26159	Remote Desktop Licensing Service の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26151	Remote Desktop のスプーフィングの脆弱性	重要	7.1	No	No	なりすまし
CVE-2026-32085	Remote Procedure Call の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-32167	SQL Server の特権昇格の脆弱性	重要	6.7	No	No	特権昇格
CVE-2026-32176	SQL Server の特権昇格の脆弱性	重要	6.7	No	No	特権昇格
CVE-2026-0390	UEFI Secure Boot のセキュリティ機能バイパスの脆弱性	重要	6.7	No	No	セキュリティ機能バイパス
CVE-2026-32220	UEFI Secure Boot のセキュリティ機能バイパスの脆弱性	重要	4.4	No	No	セキュリティ機能バイパス
CVE-2026-32212	Universal Plug and Play (upnp.dll) の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-32214	Universal Plug and Play (upnp.dll) の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-32079	Web Account Manager の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-33104	Win32k の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32196	Windows Admin Center のスプーフィングの脆弱性	重要	6.1	No	No	なりすまし
CVE-2026-26178	Windows Advanced Rasterization Platform の特権昇格の脆弱性	重要	8.8	No	No	特権昇格
CVE-2026-32073	Windows Ancillary Function Driver for WinSock の特権昇格の脆弱性	重要	7	No	No	特権昇格

CVE-2026-26168	Windows Ancillary Function Driver for WinSock の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26173	Windows Ancillary Function Driver for WinSock の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-26177	Windows Ancillary Function Driver for WinSock の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-26182	Windows Ancillary Function Driver for WinSock の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-27922	Windows Ancillary Function Driver for WinSock の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-33099	Windows Ancillary Function Driver for WinSock の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-33100	Windows Ancillary Function Driver for WinSock の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32088	Windows Biometric Service のセキュリティ機能バイパスの脆弱性	重要	6.1	No	No	セキュリティ機能バイパス
CVE-2026-27913	Windows BitLocker のセキュリティ機能バイパスの脆弱性	重要	7.7	No	No	セキュリティ機能バイパス
CVE-2026-26175	Windows Boot Manager のセキュリティ機能バイパスの脆弱性	重要	4.6	No	No	セキュリティ機能バイパス
CVE-2026-32162	Windows COM の特権昇格の脆弱性	重要	8.4	No	No	特権昇格
CVE-2026-20806	Windows COM Server の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-26176	Windows Client Side Caching driver (csc.sys) の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-27926	Windows Cloud Files Mini Filter Driver の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32070	Windows Common Log File System Driver の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-33098	Windows Container Isolation FS Filter Driver の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26153	Windows Encrypted File System (EFS) の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32087	Windows Function Discovery Service (fdwsd.dll) の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32093	Windows Function Discovery Service (fdwsd.dll) の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32086	Windows Function Discovery Service (fdwsd.dll) の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32150	Windows Function Discovery Service (fdwsd.dll) の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-27931	Windows GDI の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-27930	Windows GDI の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-32221	Windows Graphics Component のリモート コード実行の脆弱性	重要	8.4	No	No	リモートコード実行
CVE-2026-27906	Windows Hello のセキュリティ機能バイパスの脆弱性	重要	4.4	No	No	セキュリティ機能バイパス
CVE-2026-27928	Windows Hello のセキュリティ機能バイパスの脆弱性	重要	8.7	No	No	セキュリティ機能バイパス
CVE-2026-26156	Windows Hyper-V のリモート コード実行の脆弱性	重要	7.8	No	No	リモートコード実行
CVE-2026-32149	Windows Hyper-V のリモート コード実行の脆弱性	重要	7.3	No	No	リモートコード実行
CVE-2026-27910	Windows Installer の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-27912	Windows Kerberos の特権昇格の脆弱性	重要	8	No	No	特権昇格
CVE-2026-26179	Windows Kernel の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26180	Windows Kernel の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32195	Windows Kernel の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-26163	Windows Kernel の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32215	Windows Kernel の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-32217	Windows Kernel の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-32218	Windows Kernel の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩

CVE-2026-26169	Windows Kernel Memory の情報漏洩の脆弱性	重要	6.1	No	No	情報漏洩
CVE-2026-27929	Windows LUA File Virtualization Filter Driver の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32071	Windows Local Security Authority Subsystem Service (LSASS) のサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
CVE-2026-20930	Windows Management Services の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26162	Windows OLE の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-33101	Windows Print Spooler の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32084	Windows Print Spooler の情報漏洩の脆弱性	重要	5.5	No	No	情報漏洩
CVE-2026-27927	Windows Projected File System の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26184	Windows Projected File System の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32069	Windows Projected File System の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32074	Windows Projected File System の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32078	Windows Projected File System の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26167	Windows Push Notifications の特権昇格の脆弱性	重要	8.8	No	No	特権昇格
CVE-2026-32158	Windows Push Notifications の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32159	Windows Push Notifications の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32160	Windows Push Notifications の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26172	Windows Push Notifications の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-20928	Windows Recovery Environment のセキュリティ機能バイパスの脆弱性	重要	4.6	No	No	セキュリティ機能バイパス
CVE-2026-32216	Windows Redirected Drive Buffering System のサービス拒否の脆弱性	重要	5.5	No	No	DoS攻撃
CVE-2026-27909	Windows Search Service の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26161	Windows Sensor Data Service の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-26174	Windows Server Update Service (WSUS) の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32224	Windows Server Update Service (WSUS) の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-26154	Windows Server Update Service (WSUS) の改ざんの脆弱性	重要	7.5	No	No	Tampering
CVE-2026-26165	Windows Shell の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-26166	Windows Shell の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-27918	Windows Shell の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32151	Windows Shell の情報漏洩の脆弱性	重要	6.5	No	No	情報漏洩
CVE-2026-32225	Windows Shell のセキュリティ機能バイパスの脆弱性	重要	8.8	No	No	セキュリティ機能バイパス
CVE-2026-32202	Windows Shell のスプーフィングの脆弱性	重要	4.3	No	No	なりすまし
CVE-2026-32082	Windows Simple Search and Discovery Protocol (SSDP) Service の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32083	Windows Simple Search and Discovery Protocol (SSDP) Service の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32068	Windows Simple Search and Discovery Protocol (SSDP) Service の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32183	Windows Snipping Tool のリモート コード実行の脆弱性	重要	7.8	No	No	リモートコード実行
CVE-2026-32089	Windows Speech Brokered Api の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32090	Windows Speech Brokered Api の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32153	Windows Speech Runtime の特権昇格の脆弱性	重要	7.8	No	No	特権昇格

CVE-2026-27907	Windows Storage Spaces Controller の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32076	Windows Storage Spaces Controller の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-27908	Windows TDI Translation Driver (tdx.sys) の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-27921	Windows TDI Translation Driver (tdx.sys) の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-27915	Windows UPnP Device Host の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-27919	Windows UPnP Device Host の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32075	Windows UPnP Device Host の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-27916	Windows UPnP Device Host の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-27920	Windows UPnP Device Host の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32077	Windows UPnP Device Host の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-27925	Windows UPnP Device Host の情報漏洩の脆弱性	重要	6.5	No	No	情報漏洩
CVE-2026-32156	Windows UPnP Device Host のリモート コード実行の脆弱性	重要	7.4	No	No	リモートコード実行
CVE-2026-32223	Windows USB Printing Stack (usbprint.sys) の特権昇格の脆弱性	重要	6.8	No	No	特権昇格
CVE-2026-32165	Windows User Interface Core の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-27911	Windows User Interface Core の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32163	Windows User Interface Core の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-32164	Windows User Interface Core の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-23670	Windows Virtualization-Based Security (VBS) のセキュリティ機能バイパスの脆弱性	重要	5.7	No	No	セキュリティ機能バイパス
CVE-2026-27917	Windows WFP NDIS Lightweight Filter Driver (wfplwfs.sys) の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32080	Windows WalletService の特権昇格の脆弱性	重要	7	No	No	特権昇格
CVE-2026-32222	Windows Win32k の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
CVE-2026-21637 *	HackerOne: CVE-2026-21637 TLS PSK/ALPN コールバック例外によるエラーハンドラのバイパス	警告	7.5	No	No	セキュリティ機能バイパス
CVE-2026-33119	Microsoft Edge (Chromium-based) for Android のスプーフィングの脆弱性	警告	5.4	No	No	なりすまし
CVE-2026-33829	Windows Snipping Tool のスプーフィングの脆弱性	警告	4.3	No	No	なりすまし
CVE-2026-5858 *	Chromium: CVE-2026-5858 WebML におけるヒープ バッファ オーバーフロー	緊急	N/A	No	No	リモートコード実行
CVE-2026-5859 *	Chromium: CVE-2026-5859 WebML における整数オーバーフロー	緊急	N/A	No	No	リモートコード実行
CVE-2026-5272 *	Chromium: CVE-2026-5272 GPU におけるヒープ バッファ オーバーフロー	高	N/A	No	No	リモートコード実行
CVE-2026-5273 *	Chromium: CVE-2026-5273 CSS における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5274 *	Chromium: CVE-2026-5274 Codecs における整数オーバーフロー	高	N/A	No	No	リモートコード実行
CVE-2026-5275 *	Chromium: CVE-2026-5275 ANGLE におけるヒープ バッファ オーバーフロー	高	N/A	No	No	リモートコード実行
CVE-2026-5276 *	Chromium: CVE-2026-5276 WebUSB における不十分なポリシー適用	高	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5277 *	Chromium: CVE-2026-5277 ANGLE における整数オーバーフロー	高	N/A	No	No	リモートコード実行
CVE-2026-5279 *	Chromium: CVE-2026-5279 V8 におけるオブジェクト破損	高	N/A	No	No	リモートコード実行
CVE-2026-5280 *	Chromium: CVE-2026-5280 WebCodecs における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5283 *	Chromium: CVE-2026-5283 ANGLE における不適切な実装	高	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5284 *	Chromium: CVE-2026-5284 Dawn における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5285 *	Chromium: CVE-2026-5285 WebGL における解放後使用	高	N/A	No	No	リモートコード実行

CVE-2026-5286 *	Chromium: CVE-2026-5286 Dawn における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5287 *	Chromium: CVE-2026-5287 PDF における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5289 *	Chromium: CVE-2026-5289 Navigation における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5290 *	Chromium: CVE-2026-5290 Compositing における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5860 *	Chromium: CVE-2026-5860 WebRTC における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5861 *	Chromium: CVE-2026-5861 V8 における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5862 *	Chromium: CVE-2026-5862 V8 における不適切な実装	高	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5863 *	Chromium: CVE-2026-5863 V8 における不適切な実装	高	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5864 *	Chromium: CVE-2026-5864 WebAudio におけるヒープ バッファ オーバーフロー	高	N/A	No	No	リモートコード実行
CVE-2026-5865 *	Chromium: CVE-2026-5865 V8 における型混同	高	N/A	No	No	リモートコード実行
CVE-2026-5866 *	Chromium: CVE-2026-5866 Media における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5867 *	Chromium: CVE-2026-5867 WebML におけるヒープ バッファ オーバーフロー	高	N/A	No	No	リモートコード実行
CVE-2026-5868 *	Chromium: CVE-2026-5868 ANGLE におけるヒープ バッファ オーバーフロー	高	N/A	No	No	リモートコード実行
CVE-2026-5869 *	Chromium: CVE-2026-5869 WebML におけるヒープ バッファ オーバーフロー	高	N/A	No	No	リモートコード実行
CVE-2026-5870 *	Chromium: CVE-2026-5870 Skia における整数オーバーフロー	高	N/A	No	No	リモートコード実行
CVE-2026-5871 *	Chromium: CVE-2026-5871 V8 における型混同	高	N/A	No	No	リモートコード実行
CVE-2026-5872 *	Chromium: CVE-2026-5872 Blink における解放後使用	高	N/A	No	No	リモートコード実行
CVE-2026-5873 *	Chromium: CVE-2026-5873 V8 における境界外読み取りおよび書き込み	高	N/A	No	No	リモートコード実行
CVE-2026-5291 *	Chromium: CVE-2026-5291 WebGL における不適切な実装	中	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5292 *	Chromium: CVE-2026-5292 WebCodecs における境界外読み取り	中	N/A	No	No	情報漏洩
CVE-2026-5874 *	Chromium: CVE-2026-5874 PrivateAI における解放後使用	中	N/A	No	No	リモートコード実行
CVE-2026-5875 *	Chromium: CVE-2026-5875 Blink におけるポリシー バイパス	中	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5876 *	Chromium: CVE-2026-5876 Navigation におけるサイドチャネル情報漏洩	中	N/A	No	No	情報漏洩
CVE-2026-5877 *	Chromium: CVE-2026-5877 Navigation における解放後使用	中	N/A	No	No	リモートコード実行
CVE-2026-5878 *	Chromium: CVE-2026-5878 Blink における不正確なセキュリティ UI	中	N/A	No	No	なりすまし
CVE-2026-5879 *	Chromium: CVE-2026-5879 ANGLE における信頼できない入力の不十分な検証	中	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5880 *	Chromium: CVE-2026-5880 browser UI における不正確なセキュリティ UI	中	N/A	No	No	なりすまし
CVE-2026-5881 *	Chromium: CVE-2026-5881 LocalNetworkAccess におけるポリシー バイパス	中	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5882 *	Chromium: CVE-2026-5882 Fullscreen における不正確なセキュリティ UI	中	N/A	No	No	なりすまし
CVE-2026-5883 *	Chromium: CVE-2026-5883 Media における解放後使用	中	N/A	No	No	リモートコード実行
CVE-2026-5884 *	Chromium: CVE-2026-5884 Media における信頼できない入力の不十分な検証	中	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5885 *	Chromium: CVE-2026-5885 WebML における信頼できない入力の不十分な検証	中	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5886 *	Chromium: CVE-2026-5886 WebAudio における境界外読み取り	中	N/A	No	No	情報漏洩
CVE-2026-5887 *	Chromium: CVE-2026-5887 Downloads における信頼できない入力の不十分な検証	中	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5888 *	Chromium: CVE-2026-5888 WebCodecs における未初期化使用	中	N/A	No	No	リモートコード実行
CVE-2026-5889 *	Chromium: CVE-2026-5889 PDFium における暗号上の欠陥	中	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5890 *	Chromium: CVE-2026-5890 WebCodecs における競合状態	中	N/A	No	No	リモートコード実行

CVE-2026-5891 *	Chromium: CVE-2026-5891 browser UI における不十分なポリシー適用	中	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5892 *	Chromium: CVE-2026-5892 PWA における不十分なポリシー適用	中	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5893 *	Chromium: CVE-2026-5893 V8 における競合状態	中	N/A	No	No	リモートコード実行
CVE-2026-5894 *	Chromium: CVE-2026-5894 PDF における不適切な実装	低	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5895 *	Chromium: CVE-2026-5895 Omnibox における不正確なセキュリティ UI	低	N/A	No	No	なりすまし
CVE-2026-5896 *	Chromium: CVE-2026-5896 Audio におけるポリシー バイパス	低	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5897 *	Chromium: CVE-2026-5897 Downloads における不正確なセキュリティ UI	低	N/A	No	No	なりすまし
CVE-2026-5898 *	Chromium: CVE-2026-5898 Omnibox における不正確なセキュリティ UI	低	N/A	No	No	なりすまし
CVE-2026-5899 *	Chromium: CVE-2026-5899 History Navigation における不正確なセキュリティ UI	低	N/A	No	No	なりすまし
CVE-2026-5900 *	Chromium: CVE-2026-5900 Downloads におけるポリシー バイパス	低	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5901 *	Chromium: CVE-2026-5901 DevTools におけるポリシー バイパス	低	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5902 *	Chromium: CVE-2026-5902 Media における競合状態	低	N/A	No	No	リモートコード実行
CVE-2026-5903 *	Chromium: CVE-2026-5903 IFrameSandbox におけるポリシー バイパス	低	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5904 *	Chromium: CVE-2026-5904 V8 における解放後使用	低	N/A	No	No	リモートコード実行
CVE-2026-5905 *	Chromium: CVE-2026-5905 Permissions における不正確なセキュリティ UI	低	N/A	No	No	なりすまし
CVE-2026-5906 *	Chromium: CVE-2026-5906 Omnibox における不正確なセキュリティ UI	低	N/A	No	No	なりすまし
CVE-2026-5907 *	Chromium: CVE-2026-5907 Media における不十分なデータ検証	低	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5908 *	Chromium: CVE-2026-5908 Media における整数オーバーフロー	低	N/A	No	No	リモートコード実行
CVE-2026-5909 *	Chromium: CVE-2026-5909 Media における整数オーバーフロー	低	N/A	No	No	リモートコード実行
CVE-2026-5910 *	Chromium: CVE-2026-5910 Media における整数オーバーフロー	低	N/A	No	No	リモートコード実行
CVE-2026-5911 *	Chromium: CVE-2026-5911 ServiceWorkers におけるポリシー バイパス	低	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5912 *	Chromium: CVE-2026-5912 WebRTC における整数オーバーフロー	低	N/A	No	No	リモートコード実行
CVE-2026-5913 *	Chromium: CVE-2026-5913 Blink における境界外読み取り	低	N/A	No	No	情報漏洩
CVE-2026-5914 *	Chromium: CVE-2026-5914 CSS における型混同	低	N/A	No	No	リモートコード実行
CVE-2026-5915 *	Chromium: CVE-2026-5915 WebML における信頼できない入力の不十分な検証	低	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5918 *	Chromium: CVE-2026-5918 Navigation における不適切な実装	低	N/A	No	No	セキュリティ機能バイパス
CVE-2026-5919 *	Chromium: CVE-2026-5919 WebSockets における信頼できない入力の不十分な検証	低	N/A	No	No	セキュリティ機能バイパス
CVE-2026-33118	Microsoft Edge (Chromium-based) のスプーフィングの脆弱性	低	4.3	No	No	なりすまし

* は、この CVE が第三者によってすでに公開されており、今回 Microsoft の公開情報に含まれたことを示します。

† は、脆弱性に完全に対処するために追加の管理上の対応が必要であることを示します。