

	CVE番号	記述	深刻度	CVSS	周知されたか	悪用されたか	脆弱性タイプ
1	<a href="#">CVE-2024-43572</a>	Microsoft 管理コンソールにおけるリモートコード実行の脆弱性	警告	7.8	Yes	Yes	リモートコード実行
2	<a href="#">CVE-2024-43573</a>	Windows MSHTML プラットフォームのなりすましの脆弱性	警告	6.5	Yes	Yes	なりすまし
3	<a href="#">CVE-2024-6197 *</a>	オープンソースCurlリモートコード実行の脆弱性	重要	8.8	Yes	No	リモートコード実行
4	<a href="#">CVE-2024-20659</a>	Windows Hyper-V セキュリティ機能バイパスの脆弱性	重要	7.1	Yes	No	セキュリティ機能バイパス
5	<a href="#">CVE-2024-43583</a>	Winlogon 特権昇格の脆弱性	重要	7.8	Yes	No	特権昇格
6	<a href="#">CVE-2024-43468 †</a>	Microsoft Configuration Manager 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
7	<a href="#">CVE-2024-43582</a>	リモートデスクトッププロトコルサーバ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
8	<a href="#">CVE-2024-43488</a>	Visual Studio Code extension for Arduino 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
9	<a href="#">CVE-2024-43485</a>	.NET および Visual Studio におけるサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
10	<a href="#">CVE-2024-38229</a>	.NETおよびVisual Studioリモートコード実行の脆弱性	重要	8.1	No	No	リモートコード実行
11	<a href="#">CVE-2024-43483</a>	.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
12	<a href="#">CVE-2024-43484</a>	.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
13	<a href="#">CVE-2024-43591</a>	Azure コマンドライン統合 (CLI) の特権昇格の脆弱性	重要	8.7	No	No	特権昇格
14	<a href="#">CVE-2024-38097</a>	Azure Monitor Agent の特権昇格の脆弱性	重要	7.1	No	No	特権昇格
15	<a href="#">CVE-2024-43480</a>	Azure Service Fabric for Linux リモートコード実行の脆弱性	重要	6.6	No	No	リモートコード実行
16	<a href="#">CVE-2024-38179</a>	Azure Stack HCI における特権昇格の脆弱性	重要	8.8	No	No	特権昇格
17	<a href="#">CVE-2024-43513 †</a>	BitLocker セキュリティ機能バイパスの脆弱性	重要	6.4	No	No	セキュリティ機能バイパス
18	<a href="#">CVE-2024-38149</a>	BranchCache サービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
19	<a href="#">CVE-2024-43506</a>	BranchCache サービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
20	<a href="#">CVE-2024-43585</a>	Code Integrity Guard セキュリティ機能バイパスの脆弱性	重要	5.5	No	No	セキュリティ機能バイパス
21	<a href="#">CVE-2024-43497</a>	DeepSpeed 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
22	<a href="#">CVE-2024-43515</a>	Internet Small Computer Systems Interface (iSCSI) サービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
23	<a href="#">CVE-2024-43517</a>	Microsoft ActiveX データオブジェクト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
24	<a href="#">CVE-2024-43614</a>	Microsoft Defender for Endpoint for Linux スプーフィング脆弱性	重要	5.5	No	No	なりすまし
25	<a href="#">CVE-2024-43504</a>	Microsoft Excel 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
26	<a href="#">CVE-2024-43576</a>	Microsoft Office 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
27	<a href="#">CVE-2024-43616</a>	Microsoft Office 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
28	<a href="#">CVE-2024-43609</a>	Microsoft Office スプーフィング脆弱性	重要	6.5	No	No	なりすまし
29	<a href="#">CVE-2024-43505</a>	Microsoft Office Visio 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
30	<a href="#">CVE-2024-38029</a>	Microsoft OpenSSH for Windows リモートコード実行の脆弱性	重要	7.5	No	No	リモートコード実行
31	<a href="#">CVE-2024-43581</a>	Microsoft OpenSSH for Windows リモートコード実行の脆弱性	重要	7.1	No	No	リモートコード実行
32	<a href="#">CVE-2024-43615</a>	Microsoft OpenSSH for Windows リモートコード実行の脆弱性	重要	7.1	No	No	リモートコード実行
33	<a href="#">CVE-2024-43503</a>	Microsoft SharePoint における特権昇格の脆弱性	重要	7.8	No	No	特権昇格
34	<a href="#">CVE-2024-43541</a>	Microsoft Simple Certificate Enrollment Protocol にサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
35	<a href="#">CVE-2024-43544</a>	Microsoft Simple Certificate Enrollment Protocol サービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
36	<a href="#">CVE-2024-43574</a>	Microsoft Speech Application Programming Interface (SAPI) リモートコード実行の脆弱性	重要	8.3	No	No	リモートコード実行
37	<a href="#">CVE-2024-43519</a>	Microsoft WDAC OLE DB provider for SQL Server 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

38	<a href="#">CVE-2024-43560</a>	Microsoft Windows Storage Port Driver における特権昇格の脆弱性	重要	7.8	No	No	特権昇格
39	<a href="#">CVE-2024-43553</a>	NT OS カーネルの特権昇格の脆弱性	重要	7.4	No	No	特権昇格
40	<a href="#">CVE-2024-43604</a>	Outlook for Android における特権昇格の脆弱性	重要	5.7	No	No	特権昇格
41	<a href="#">CVE-2024-43481</a>	Power BI レポートサーバなりすましの脆弱性	重要	6.5	No	No	なりすまし
42	<a href="#">CVE-2024-43612</a>	Power BI レポートサーバなりすましの脆弱性	重要	7.6	No	No	なりすまし
43	<a href="#">CVE-2024-43533</a>	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	重要	8.8	No	No	リモートコード実行
44	<a href="#">CVE-2024-43599</a>	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	重要	8.8	No	No	リモートコード実行
45	<a href="#">CVE-2024-43532</a>	RPC Endpoint Mapper サービスにおける特権昇格の脆弱性	重要	8.8	No	No	特権昇格
46	<a href="#">CVE-2024-43571</a>	Sudo for Windows なりすましの脆弱性	重要	5.6	No	No	なりすまし
47	<a href="#">CVE-2024-43590</a>	Visual C++ 再頒布可能インストーラの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
48	<a href="#">CVE-2024-43601</a>	Visual Studio Code for Linux リモートコード実行の脆弱性	重要	7.1	No	No	リモートコード実行
49	<a href="#">CVE-2024-43603</a>	Visual Studio コレクターサービスサービス拒否の脆弱性	重要	5.5	No	No	DoS攻撃
50	<a href="#">CVE-2024-43563</a>	WinSock 用 Windows 補助機能ドライバに特権昇格の脆弱性	重要	7.8	No	No	特権昇格
51	<a href="#">CVE-2024-43501</a>	Windows 共通ログファイルシステムドライバに特権昇格の脆弱性	重要	7.8	No	No	特権昇格
52	<a href="#">CVE-2024-43546</a>	Windows 暗号情報漏えいの脆弱性	重要	5.6	No	No	情報漏えい
53	<a href="#">CVE-2024-43509</a>	Windows グラフィックコンポーネントの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
54	<a href="#">CVE-2024-43556</a>	Windows グラフィックコンポーネントの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
55	<a href="#">CVE-2024-43508</a>	Windows グラフィック コンポーネント情報漏えいの脆弱性	重要	5.5	No	No	情報漏えい
56	<a href="#">CVE-2024-43534</a>	Windows グラフィックコンポーネント情報漏えいの脆弱性	重要	6.5	No	No	情報漏えい
57	<a href="#">CVE-2024-43521</a>	Windows Hyper-V サービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
58	<a href="#">CVE-2024-43567</a>	Windows Hyper-V サービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
59	<a href="#">CVE-2024-43575</a>	Windows Hyper-V サービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
60	<a href="#">CVE-2024-30092</a>	Windows Hyper-V リモートコード実行の脆弱性	重要	8	No	No	リモートコード実行
61	<a href="#">CVE-2024-38129</a>	Windows Kerberos における特権昇格の脆弱性	重要	7.5	No	No	特権昇格
62	<a href="#">CVE-2024-43547</a>	Windows Kerberos 情報漏えいの脆弱性	重要	6.5	No	No	情報漏えい
63	<a href="#">CVE-2024-43520</a>	Windowsカーネルサービス拒否の脆弱性	重要	5	No	No	DoS攻撃
64	<a href="#">CVE-2024-37979</a>	Windows カーネルの特権昇格の脆弱性	重要	6.7	No	No	特権昇格
65	<a href="#">CVE-2024-43502</a>	Windows カーネルの特権昇格の脆弱性	重要	7.1	No	No	特権昇格
66	<a href="#">CVE-2024-43511</a>	Windows カーネルの特権昇格の脆弱性	重要	7	No	No	特権昇格
67	<a href="#">CVE-2024-43527</a>	Windows カーネルの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
68	<a href="#">CVE-2024-43570</a>	Windows カーネル特権昇格の脆弱性	重要	6.4	No	No	特権昇格
69	<a href="#">CVE-2024-43535</a>	Windows カーネルモードドライバの特権昇格の脆弱性	重要	7	No	No	特権昇格
70	<a href="#">CVE-2024-43554</a>	Windows カーネルモードドライバ情報漏えいの脆弱性	重要	5.5	No	No	情報漏えい
71	<a href="#">CVE-2024-43522</a>	Windows ローカルセキュリティ権限 (LSA) の特権昇格の脆弱性	重要	7	No	No	特権昇格
72	<a href="#">CVE-2024-43537</a>	Windows Mobile Broadband ドライバにサービス拒否の脆弱性	重要	6.5	No	No	DoS攻撃
73	<a href="#">CVE-2024-43538</a>	Windows Mobile ブロードバンド ドライバのサービス拒否の脆弱性	重要	6.5	No	No	DoS攻撃
74	<a href="#">CVE-2024-43540</a>	Windows Mobile ブロードバンド ドライバのサービス拒否の脆弱性	重要	6.5	No	No	DoS攻撃
75	<a href="#">CVE-2024-43542</a>	Windows Mobile ブロードバンド ドライバのサービス拒否の脆弱性	重要	6.5	No	No	DoS攻撃

76	<a href="#">CVE-2024-43555</a>	Windows Mobile ブロードバンド ドライバのサービス拒否の脆弱性	重要	6.5	No	No	DoS攻撃
77	<a href="#">CVE-2024-43557</a>	Windows Mobile ブロードバンド ドライバのサービス拒否の脆弱性	重要	6.5	No	No	DoS攻撃
78	<a href="#">CVE-2024-43558</a>	Windows Mobile ブロードバンド ドライバのサービス拒否の脆弱性	重要	6.5	No	No	DoS攻撃
79	<a href="#">CVE-2024-43559</a>	Windows Mobile ブロードバンド ドライバのサービス拒否の脆弱性	重要	6.5	No	No	DoS攻撃
80	<a href="#">CVE-2024-43561</a>	Windows Mobile ブロードバンド ドライバのサービス拒否の脆弱性	重要	6.5	No	No	DoS攻撃
81	<a href="#">CVE-2024-43523</a>	Windows Mobile Broadband ドライバのリモートコード実行の脆弱性	重要	6.8	No	No	リモートコード実行
82	<a href="#">CVE-2024-43524</a>	Windows Mobile Broadband ドライバのリモートコード実行の脆弱性	重要	6.8	No	No	リモートコード実行
83	<a href="#">CVE-2024-43525</a>	Windows Mobile Broadband ドライバのリモートコード実行の脆弱性	重要	6.8	No	No	リモートコード実行
84	<a href="#">CVE-2024-43526</a>	Windows Mobile Broadband ドライバのリモートコード実行の脆弱性	重要	6.8	No	No	リモートコード実行
85	<a href="#">CVE-2024-43536</a>	Windows Mobile Broadband ドライバのリモートコード実行の脆弱性	重要	6.8	No	No	リモートコード実行
86	<a href="#">CVE-2024-43543</a>	Windows Mobile Broadband ドライバのリモートコード実行の脆弱性	重要	6.8	No	No	リモートコード実行
87	<a href="#">CVE-2024-38124</a>	Windows ネットログオンの特権昇格の脆弱性	重要	9	No	No	特権昇格
88	<a href="#">CVE-2024-43562</a>	Windows ネットワークアドレス変換 (NAT) サービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
89	<a href="#">CVE-2024-43565</a>	Windows ネットワークアドレス変換 (NAT) サービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
90	<a href="#">CVE-2024-43545</a>	Windows オンライン証明書ステータスプロトコル(OCSP)サーバのサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
91	<a href="#">CVE-2024-43529</a>	Windows Print Spooler における特権昇格の脆弱性	重要	7.3	No	No	特権昇格
92	<a href="#">CVE-2024-38262</a>	Windows リモートデスクトップライセンスサービスリモートコード実行の脆弱性	重要	7.5	No	No	リモートコード実行
93	<a href="#">CVE-2024-43456</a>	Windows リモートデスクトップサービス改ざんの脆弱性	重要	4.8	No	No	改ざん
94	<a href="#">CVE-2024-43514</a>	Windows レジリエントファイルシステム(ReFS)の特権昇格の脆弱性	重要	7.8	No	No	特権昇格
95	<a href="#">CVE-2024-43500</a>	Windows Resilient File System (ReFS) 情報漏えいの脆弱性	重要	5.5	No	No	情報漏えい
96	<a href="#">CVE-2024-37976</a>	Windows Resume Extensible Firmware Interface 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
97	<a href="#">CVE-2024-37982</a>	Windows Resume Extensible Firmware Interface 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
98	<a href="#">CVE-2024-37983</a>	Windows Resume Extensible Firmware Interface 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
99	<a href="#">CVE-2024-38212</a>	Windows Routing and Remote Access Service (RRAS) 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
100	<a href="#">CVE-2024-38261</a>	Windows Routing and Remote Access Service (RRAS) 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
101	<a href="#">CVE-2024-38265</a>	Windows Routing and Remote Access Service (RRAS) 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
102	<a href="#">CVE-2024-43453</a>	Windows Routing and Remote Access Service (RRAS) 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
103	<a href="#">CVE-2024-43549</a>	Windows Routing and Remote Access Service (RRAS) 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
104	<a href="#">CVE-2024-43564</a>	Windows Routing and Remote Access Service (RRAS) 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
105	<a href="#">CVE-2024-43589</a>	Windows Routing and Remote Access Service (RRAS) 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
106	<a href="#">CVE-2024-43592</a>	Windows Routing and Remote Access Service (RRAS) 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
107	<a href="#">CVE-2024-43593</a>	Windows Routing and Remote Access Service (RRAS) 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
108	<a href="#">CVE-2024-43607</a>	Windows Routing and Remote Access Service (RRAS) 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
109	<a href="#">CVE-2024-43608</a>	Windows Routing and Remote Access Service (RRAS) 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
110	<a href="#">CVE-2024-43611</a>	Windows Routing and Remote Access Service (RRAS) 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
111	<a href="#">CVE-2024-43584</a>	Windows スクリプトエンジン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
112	<a href="#">CVE-2024-43550</a>	Windows Secure Channel スプーフィングの脆弱性	重要	7.4	No	No	なりすまし
113	<a href="#">CVE-2024-43516</a>	Windows Secure Kernel Mode における特権昇格の脆弱性	重要	7.8	No	No	特権昇格
114	<a href="#">CVE-2024-43528</a>	Windows セキュアカーネルモード特権昇格の脆弱性	重要	7.8	No	No	特権昇格
115	<a href="#">CVE-2024-43552</a>	Windows シェル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

116	<a href="#">CVE-2024-43512</a>	Windows 標準ベースのストレージ管理サービスのサービス拒否の脆弱性	重要	6.5	No	No	DoS攻撃
117	<a href="#">CVE-2024-43551</a>	Windows Storage における特権昇格の脆弱性	重要	7.8	No	No	特権昇格
118	<a href="#">CVE-2024-43518</a>	Windows テレフォニーサーバー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
119	<a href="#">CVE-2024-7025 *</a>	Chromium CVE-2024-7025 Layout 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
120	<a href="#">CVE-2024-9369 *</a>	Chromium CVE-2024-9369 Mojo におけるデータ検証の不備	高	N/A	No	No	リモートコード実行
121	<a href="#">CVE-2024-9370 *</a>	Chromium CVE-2024-9370 V8 における不適切な実装	高	N/A	No	No	リモートコード実行

\*サードパーティによってリリースされ、現在Microsoftのリリースに含まれていることを示す。

†脆弱性に完全に対処するために、インストール後の対応が必要であることを示す。