	CVE番号	名称	深刻度	CVSS	公開されたか	悪用されたか	脆弱性タイプ
1	CVE-2023-28252	Windows Common Log File System Driverの特権昇格の脆弱性	重要	7.8	No	Yes	特権昇格
2	CVE-2023-28231	DHCP Server Service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
3	CVE-2023-28219	Layer 2 Tunneling Protocol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
4	CVE-2023-28220	Layer 2 Tunneling Protocol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
5	CVE-2023-21554	Microsoft Message Queuing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
6	CVE-2023-28291	Raw Image Extension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
7	CVE-2023-28232	Windows Point-to-Point Tunneling Protocolのリモートコード実行の脆弱性	緊急	7.5	No	No	リモートコード実行
8	CVE-2023-28250	Windows Pragmatic General Multicast (PGM)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
9	CVE-2023-28260	.NET DLL Hijackingによる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
10	CVE-2023-28312	Azure Machine Learningの情報漏えいの脆弱性	重要	6.5	No	No	情報漏えい
11	CVE-2023-28300	Azure Service Connectorのセキュリティ機能バイパスの脆弱性	重要	7.5	No	No	セキュリティ機能バイパス
12	CVE-2023-24860	Microsoft DefenderのDenial of Serviceの脆弱性	重要	7.5	No	No	DoS攻撃
13	CVE-2023-28309	Microsoft Dynamics 365 (オンプレミス) のクロスサイトスクリプティングの脆弱性	重要	7.6	No	No	クロスサイトスクリプティング
14	CVE-2023-28314	Microsoft Dynamics 365 (オンプレミス) のクロスサイトスクリプティングの脆弱性	重要	6.1	No	No	クロスサイトスクリプティング
15	CVE-2023-28313	Microsoft Dynamics 365 Customer Voiceのクロスサイトスクリプティングの脆弱性	重要	6.1	No	No	クロスサイトスクリプティング
16	CVE-2023-21769	Microsoft Message Queuing Denial of Service 脆弱性	重要	7.5	No	No	DoS攻撃
17	CVE-2023-28302	Microsoft Message Queuing Denial of Service 脆弱性	重要	7.5	No	No	DoS攻撃
18	CVE-2023-28285	Microsoft Office Graphics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
19	CVE-2023-24883	Microsoft PostScript and PCL6 Class Printer Driver 情報公開の脆弱性	重要	6.5	No	No	情報漏えい
20	CVE-2023-24884	Microsoft PostScript and PCL6 Class Printer Driver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
21	CVE-2023-24885	Microsoft PostScript and PCL6 Class Printer Driver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
22	CVE-2023-24886	Microsoft PostScript and PCL6 Class Printer Driver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
23	CVE-2023-24887	Microsoft PostScript and PCL6 Class Printer Driver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	CVE-2023-24924	Microsoft PostScript and PCL6 Class Printer Driver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
25	CVE-2023-24925	Microsoft PostScript and PCL6 Class Printer Driver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
26	CVE-2023-24926	Microsoft PostScript and PCL6 Class Printer Driver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
27	CVE-2023-24927	Microsoft PostScript and PCL6 Class Printer Driver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
28	CVE-2023-24928	Microsoft PostScript and PCL6 Class Printer Driver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
29	CVE-2023-24929	Microsoft PostScript and PCL6 Class Printer Driver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
30	CVE-2023-28243	Microsoft PostScript and PCL6 Class Printer Driver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
31	CVE-2023-28287	Microsoft Publisher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
32	CVE-2023-28295	Microsoft Publisher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
33	CVE-2023-28288	Microsoft SharePoint Server のなりすましの脆弱性	重要	6.5	No	No	なりすまし
34	CVE-2023-23375	Microsoft SQL Server 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
35	CVE-2023-23384	Microsoft SQL Server 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
36	CVE-2023-28304	Microsoft SQL Server 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
37	CVE-2023-28275	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	CVE-2023-28311	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
39	CVE-2023-28268	Netlogon RPCによる特権の昇格の脆弱性	重要	8.1	No	No	特権昇格

40	CVE-2023-28292	Raw Image Extension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
41	CVE-2023-28267	リモートデスクトッププロトコルクライアント情報漏えいの脆弱性	重要	6.5	No	No	情報漏えい
42	CVE-2023-21729	リモートプロシージャコール実行時の情報漏えいの脆弱性	重要	4.3	No	No	情報漏えい
43	CVE-2023-21727	リモートプロシージャコールランタイム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	CVE-2023-24893	Visual Studio Code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
45	CVE-2023-28262	Visual Studioの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
46	CVE-2023-28263	Visual Studioの情報漏洩の脆弱性	重要	5.5	No	No	情報漏えい
47	CVE-2023-28296	Visual Studio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
48	CVE-2023-28299	Visual Studioのなりすましの脆弱性	重要	5.5	No	No	なりすまし
49	CVE-2023-24914	Win32k 権限昇格の脆弱性	重要	7	No	No	特権昇格
50	CVE-2023-28223	Windows Domain Name Serviceの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
51	CVE-2023-28216	Windows Advanced Local Procedure Call (ALPC) 権限昇格の脆弱性	重要	7	No	No	特権昇格
52	CVE-2023-28218	WindowsのWinSock用補助機能ドライバに特権昇格の脆弱性	重要	7	No	No	特権昇格
53	CVE-2023-28227	Windows Bluetoothドライバの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
54	CVE-2023-28249	Windows Boot Managerのセキュリティ機能回避の脆弱性	重要	6.6	No	No	セキュリティ機能バイパス
55	CVE-2023-28269	Windows Boot Managerのセキュリティ機能回避の脆弱性	重要	6.8	No	No	セキュリティ機能バイパス
56	CVE-2023-28273	Windows Clip Serviceの特権昇格の脆弱性	重要	7	No	No	特権昇格
57	CVE-2023-28229	Windows CNGキーアイソレーションサービスによる特権昇格の脆弱性	重要	7	No	No	特権昇格
58	CVE-2023-28266	Windowsコモンログファイルシステムドライバ情報漏えいの脆弱性	重要	5.5	No	No	情報漏えい
59	CVE-2023-28277	Windows DNSサーバの情報漏えいの脆弱性	重要	4.9	No	No	情報漏えい
60	CVE-2023-28254	Windows DNSサーバーのリモートコード実行の脆弱性	重要	7.2	No	No	リモートコード実行
61	CVE-2023-28255	Windows DNSサーバーの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
62	CVE-2023-28256	Windows DNSサーバーの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
63	CVE-2023-28278	Windows DNSサーバーの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
64	CVE-2023-28305	Windows DNSサーバーの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
65	CVE-2023-28306	Windows DNSサーバーの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
66	CVE-2023-28307	Windows DNSサーバーの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
67	CVE-2023-28308	Windows DNSサーバーの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
68	CVE-2023-28226	Windows Enroll Engineのセキュリティ機能回避の脆弱性	重要	5.3	No	No	セキュリティ機能バイパス
69	CVE-2023-28221	Windows Error Reporting Serviceの特権昇格の脆弱性	重要	7	No	No	特権昇格
70	CVE-2023-24912	Windows Graphics Componentの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
71	CVE-2023-28276	Windowsグループポリシー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
72	CVE-2023-28238	Windows Internet Key Exchange (IKE) Protocol Extensionsの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
73	CVE-2023-28244	Windows Kerberosの特権昇格の脆弱性	重要	8.1	No	No	特権昇格
74	CVE-2023-28298	Windows カーネルサービス拒否の脆弱性	重要	5.5	No	No	DoS攻撃
75	CVE-2023-28222	Windowsカーネルの特権昇格の脆弱性	重要	7.1	No	No	特権昇格
76	CVE-2023-28236	Windowsカーネルの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
77	CVE-2023-28248	Windowsカーネルの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
78	CVE-2023-28272	Windowsカーネルの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
79	CVE-2023-28293	Windowsカーネルの特権昇格の脆弱性	重要	7.8	No	No	特権昇格

80	CVE-2023-28253	Windowsカーネル情報漏洩の脆弱性	重要	5.5	No	No	情報漏えい
81	CVE-2023-28271	Windows Kernelのメモリ情報漏洩の脆弱性	重要	5.5	No	No	情報漏えい
82	CVE-2023-28237	Windows Kernel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
83	CVE-2023-28235	Windows ロック画面のセキュリティ機能回避の脆弱性	重要	6.8	No	No	セキュリティ機能バイパス
84	CVE-2023-28270	Windows ロック画面のセキュリティ機能回避の脆弱性	重要	6.8	No	No	セキュリティ機能バイパス
85	CVE-2023-28217	Windows ネットワークアドレス変換 (NAT) のサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
86	CVE-2023-28247	Windowsネットワークファイルシステム情報漏洩の脆弱性	重要	7.5	No	No	情報漏えい
87	CVE-2023-28240	Windows ネットワークロードバランシング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
88	CVE-2023-28225	Windows NTLMによる特権昇格の脆弱性	重要	7.8	No	No	特権昇格
89	CVE-2023-28224	Windows Point-to-Point Protocol over Ethernet (PPPoE) の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
90	CVE-2023-28246	Windowsレジストリの特権昇格の脆弱性	重要	7.8	No	No	特権昇格
91	CVE-2023-28297	Windows Remote Procedure Call Service (RPCSS) の特権昇格の脆弱性	重要	8.8	No	No	特権昇格
92	CVE-2023-24931	Windows Secure Channelのサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
93	CVE-2023-28233	Windows Secure Channelのサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
94	CVE-2023-28234	Windows Secure Channelのサービス拒否の脆弱性	重要	7.5	No	No	DoS攻撃
95	CVE-2023-28241	Windows Secure Socket Tunneling Protocol (SSTP) のサービス不能の脆弱性	重要	7.5	No	No	DoS攻撃
96	CVE-2023-28228	Windowsのなりすまし脆弱性	重要	5.5	No	No	なりすまし
97	CVE-2023-28274	Windows Win32k 特権昇格の脆弱性	重要	7.8	No	No	特権昇格
98	CVE-2023-28284 *	Microsoft Edge（Chromiumベース）のセキュリティ機能回避の脆弱性について	中	4.3	No	No	セキュリティ機能バイパス
99	CVE-2023-24935 *	Microsoft Edge（Chromiumベース）のなりすましの脆弱性について	低	N/A	No	No	なりすまし
100	CVE-2023-28301 *	Microsoft Edge（Chromiumベース）の改ざんの脆弱性	低	4.2	No	No	改ざん

* このCVEが本日以前にリリースされていたことを示します。