2021 年 4 月の Microsoft 更新プログラムで対処している脆弱性一覧

CVE 識別番号	脆弱性名称	深刻度	CVSS	一般公開	悪用確認	DOS
CVE-2021-28310	Win32k 特権昇格の脆弱性	重要	7.8	いいえ	はい	EoP
CVE-2021-28458	Azure ms-rest-nodeauth ライブラリの特権昇格の脆弱性	重要	7.8	はい	いいえ	EoP
CVE-2021-27091	RPC Endpoint Mapper Service の特権昇格の脆弱性	重要	7.8	はい	いいえ	EoP
CVE-2021-28437	Windows Installer の情報漏えいの脆弱性	重要	5.5	はい	いいえ	Info
CVE-2021-28312	Windows NTFS のサービス拒否の 脆弱性	警告	3.3	はい	いいえ	DoS
CVE-2021-28460	Azure Sphere の未署名のコード実行の脆弱性	緊急	8.1	いいえ	いいえ	RCE
CVE-2021-28480	Microsoft Exchange Server のリモートコード実行の脆弱性	緊急	9.8	いいえ	いいえ	RCE
CVE-2021-28481	Microsoft Exchange Server のリモートコード実行の脆弱性	緊急	9.8	いいえ	いいえ	RCE
CVE-2021-28482	Microsoft Exchange Server のリモートコード実行の脆弱性	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28483	Microsoft Exchange Server のリモートコード実行の脆弱性	緊急	9	いいえ	いいえ	RCE

CVE-2021-28329	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28330	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28331	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28332	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28333	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28334	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28335	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28336	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28337	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28338	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	緊急	8.8	いいえ	いいえ	RCE

CVE-2021-28339	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-28343	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	緊急	8.8	いいえ	いいえ	RCE
CVE-2021-27095	Windows Media Video Decoder のリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	RCE
CVE-2021-28315	Windows Media Video Decoder のリモートコード実行の脆弱性	緊急	7.8	いいえ	いいえ	RCE
CVE-2021-27092	Azure AD Web Sign-in のセキュリティ機能バイパスの脆弱性	重要	4.3	いいえ	いいえ	SFB
CVE-2021-27067	Azure DevOps Server and Team Foundation Server の情報漏えいの脆弱性	重要	6.5	いいえ	いいえ	Info
CVE-2021-28459	Azure DevOps Server and Team Foundation Services のなりすましの脆弱性	重要	6.1	いいえ	いいえ	Spoofing
CVE-2021-28313	Diagnostics Hub Standard Collector Service の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-28321	Diagnostics Hub Standard Collector Service の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP

CVE-2021-28322	Diagnostics Hub Standard Collector Service の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-28456	Microsoft Excel の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-28451	Microsoft Excel のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28454	Microsoft Excel のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-27089	Microsoft Internet Messaging API のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28449	Microsoft Office のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28452	Microsoft Outlook のメモリ破損の脆弱性	重要	7.1	いいえ	いいえ	RCE
CVE-2021-28450	Microsoft SharePoint のサービス拒否の脆弱性	重要	5	いいえ	いいえ	DoS
CVE-2021-28317	Microsoft Windows Codecs ライブラリの情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-28453	Microsoft Word のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-27096	NTFS の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP

CVE-2021-28466	Raw Image Extension のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28468	Raw Image Extension のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28471	Remote Development Extension for Visual Studio Code のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28327	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	いいえ	いいえ	RCE
CVE-2021-28340	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	いいえ	いいえ	RCE
CVE-2021-28341	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	いいえ	いいえ	RCE
CVE-2021-28342	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	いいえ	いいえ	RCE
CVE-2021-28344	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	いいえ	いいえ	RCE
CVE-2021-28345	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	いいえ	いいえ	RCE
CVE-2021-28346	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	いいえ	いいえ	RCE

CVE-2021-28352	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	いいえ	いいえ	RCE
CVE-2021-28353	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	いいえ	いいえ	RCE
CVE-2021-28354	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	いいえ	いいえ	RCE
CVE-2021-28355	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	いいえ	いいえ	RCE
CVE-2021-28356	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	いいえ	いいえ	RCE
CVE-2021-28357	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	いいえ	いいえ	RCE
CVE-2021-28358	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	いいえ	いいえ	RCE
CVE-2021-28434	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	いいえ	いいえ	RCE
CVE-2021-28470	Visual Studio Code GitHub Pull Requests and Issues Extension のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28448	Visual Studio Code Kubernetes Tools の	重要	7.8	いいえ	いいえ	RCE

	リモートコード実行の脆弱性					
CVE-2021-28472	Visual Studio Code Maven for Java Extension のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28457	Visual Studio Code のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28469	Visual Studio Code のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28473	Visual Studio Code のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28475	Visual Studio Code のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28477	Visual Studio Code のリモートコード実行の脆弱性	重要	7	いいえ	いいえ	RCE
CVE-2021-27064	Visual Studio Installer 特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-28464	VP9 Video Extensions のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-27072	Win32k 特権昇格の脆弱性	重要	7	いいえ	いいえ	EoP
CVE-2021-28311	Windows Application Compatibility Cache	重要	6.5	いいえ	いいえ	DoS

	のサービス拒否の 脆弱性					
CVE-2021-28326	Windows AppX Deployment Server のサービス拒否の 脆弱性	重要	5.5	いいえ	いいえ	DoS
CVE-2021-28438	Windows Console Driver のサービス拒否の 脆弱性	重要	5.5	いいえ	いいえ	DoS
CVE-2021-28443	Windows Console Driver のサービス拒否の 脆弱性	重要	5.5	いいえ	いいえ	DoS
CVE-2021-28323	Windows DNS の情報漏えいの脆弱性	重要	6.5	いいえ	いいえ	Info
CVE-2021-28328	Windows DNS の情報漏えいの脆弱性	重要	6.5	いいえ	いいえ	Info
CVE-2021-27094	Windows Early Launch Antimalware Driver のセキュリティ機能バイパスの脆弱性	重要	4.4	いいえ	いいえ	SFB
CVE-2021-28447	Windows Early Launch Antimalware Driver のセキュリティ機能バイパスの脆弱性	重要	4.4	いいえ	いいえ	SFB
CVE-2021-27088	Windows Event Tracing の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-28435	Windows Event Tracing の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info

CVE-2021-28318	Windows GDI+ の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-28348	Windows GDI+ のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28349	Windows GDI+ のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-28350	Windows GDI+ のリモートコード実行の脆弱性	重要	7.8	いいえ	いいえ	RCE
CVE-2021-26416	Windows Hyper-V のサービス拒否の 脆弱性	重要	7.7	いいえ	いいえ	DoS
CVE-2021-28314	Windows Hyper-V 特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-28441	Windows Hyper-V の情報漏えいの脆弱性	重要	6.5	いいえ	いいえ	Info
CVE-2021-28444	Windows Hyper-V のセキュリティ機能バイパスの脆弱性	重要	5.7	いいえ	いいえ	SFB
CVE-2021-26415	Windows インストーラの特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-28440	Windows インストーラ特権昇格の脆弱性	重要	7	いいえ	いいえ	EoP
CVE-2021-26413	Windows インストーラのなりすましの脆弱性	重要	6.2	いいえ	いいえ	Spoofing
CVE-2021-27093	Windows カーネルの情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-28309	Windows カーネルの情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info

CVE-2021-27079	Windows Media Photo Codec の情報漏えいの脆弱性	重要	5.7	いいえ	いいえ	Info
CVE-2021-28445	Windows Network File System のリモートコード実行の脆弱性	重要	8.1	いいえ	いいえ	RCE
CVE-2021-26417	Windows Overlay Filter の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-28446	Windows ポートマッピングの情報漏えいの脆弱性	重要	7.1	いいえ	いいえ	Info
CVE-2021-28320	Windows Resource Manager PSM Service Extension の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-27090	Windows Secure Kernel Mode の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-27086	Windows Services and Controller App 特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-28324	Windows SMB の情報漏えいの脆弱性	重要	7.5	いいえ	いいえ	Info
CVE-2021-28325	Windows SMB の情報漏えいの脆弱性	重要	6.5	いいえ	いいえ	Info
CVE-2021-28347	Windows Speech Runtime 特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-28351	Windows Speech Runtime 特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP

CVE-2021-28436	Windows Speech Runtime 特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-28319	Windows TCP/IP Driver のサービス拒否の 脆弱性	重要	7.5	いいえ	いいえ	DoS
CVE-2021-28439	Windows TCP/IP Driver のサービス拒否の 脆弱性	重要	7.5	いいえ	いいえ	DoS
CVE-2021-28442	Windows TCP/IP の情報漏えいの脆弱性	重要	6.5	いいえ	いいえ	Info
CVE-2021-28316	Windows WLAN AutoConfig Service のセキュリティ機能バイパスの脆弱性	重要	4.2	いいえ	いいえ	SFB

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com