2021 年 7 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	種類
CVE-2021-34527	Windows Print Spooler のリモートコード実行の脆弱性	緊急	8.8	はい	はい	RCE
CVE-2021-34448	スクリプトエンジンのメモリ破損の脆弱性	緊急	6.8	いいえ	はい	RCE
CVE-2021-31979	Windows カーネルの特権昇格の脆弱性	重要	7.8	いいえ	はい	EoP
CVE-2021-33771	Windows カーネルの特権昇格の脆弱性	重要	7.8	いいえ	はい	EoP
CVE-2021-34473	Microsoft Exchange Server のリモートコード実行の脆弱性	緊急	9.1	はい	いいえ	RCE
CVE-2021-33781	Active Directory のセキュリティ機能バイパスの脆弱性	重要	8.1	はい	いいえ	SFB
CVE-2021-34523	Microsoft Exchange Server の特権昇格の脆弱性	重要	9	はい	いいえ	EoP
CVE-2021-33779	Windows ADFS のセキュリティ機能バイパスの脆弱性	重要	8.1	はい	いいえ	SFB
CVE-2021-34492	Windows Certificate のなりすましの脆弱性	重要	8.1	はい	いいえ	Spoofing
CVE-2021-34474	Dynamics Business Central のリモートコード実行の脆弱性	緊急	8	いいえ	いいえ	RCE
CVE-2021-34464	Microsoft Defender 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-2021-34522	Microsoft Defender 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-2021-34439	Microsoft Windows Media Foundation 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-2021-34503	Microsoft Windows Media Foundation 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-2021-34494	Windows DNS 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-2021-34450	Windows Hyper-V のリモートコード実行の脆弱性	緊急	8.5	いいえ	いいえ	RCE
CVE-2021-34458	Windows カーネル のリモートコード実行の脆弱性	緊急	9.9	いいえ	いいえ	RCE
CVE-2021-33740	Windows Media 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-2021-34497	Windows MSHTML Platform のリモートコード実行の脆弱性	緊急	6.8	いいえ	いいえ	RCE
CVE-2021-34476	Bowser.sys のサービス拒否の脆弱性	重要	7.5	いいえ	いいえ	DoS
CVE-2021-34489	DirectWrite 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-2021-34440	GDI+ の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-31947	HEVC 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-2021-33775	HEVC 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-2021-33776	HEVC 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-2021-33777	HEVC 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-2021-33778	HEVC 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-2021-33760	Media Foundation の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info

CVE-2021-33753	Microsoft Bing Search のなりすましの脆弱性	重要	4.7	いいえ	いいえ	Spoofing
CVE-2021-34501	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-2021-34518	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-2021-33766	Microsoft Exchange の情報漏えいの脆弱性	重要	7.3	いいえ	いいえ	Info
CVE-2021-33768	Microsoft Exchange Server の特権昇格の脆弱性	重要	8	いいえ	いいえ	EoP
CVE-2021-34470	Microsoft Exchange Server の特権昇格の脆弱性	重要	8	いいえ	いいえ	EoP
CVE-2021-31196	Microsoft Exchange Server のリモートコード実行の脆弱性	重要	7.2	いいえ	いいえ	RCE
CVE-2021-31206	Microsoft Exchange Server のリモートコード実行の脆弱性	重要	7.6	いいえ	いいえ	RCE
CVE-2021-34451	Microsoft Office Online Server のなりすましの脆弱性	重要	5.3	いいえ	いいえ	Spoofing
CVE-2021-34469	Microsoft Office のセキュリティ機能バイパスの脆弱性	重要	8.2	いいえ	いいえ	SFB
CVE-2021-34467	Microsoft SharePoint Server のリモートコード実行の脆弱性	重要	7.1	いいえ	いいえ	RCE
CVE-2021-34468	Microsoft SharePoint Server のリモートコード実行の脆弱性	重要	7.1	いいえ	いいえ	RCE
CVE-2021-34520	Microsoft SharePoint Server 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-2021-34517	Microsoft SharePoint Server のなりすましの脆弱性	重要	5.3	いいえ	いいえ	Spoofing

CVE-2021-34479	Microsoft Visual Studio のなりすましの脆弱性	重要	7.8	いいえ	いいえ	Spoofing
CVE-2021-34441	Microsoft Windows Media Foundation 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-2021-34452	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-2021-33767	Open Enclave SDK の特権昇格の脆弱性	重要	8.2	いいえ	いいえ	EoP
CVE-2021-31984	Power BI のリモートコード実行の脆弱性	重要	7.6	いいえ	いいえ	RCE
CVE-2021-34521	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-2021-33751	Storage Spaces Controller の特権昇格の脆弱性	重要	7	いいえ	いいえ	EoP
CVE-2021-34460	Storage Spaces Controller の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34510	Storage Spaces Controller の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34512	Storage Spaces Controller の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34513	Storage Spaces Controller の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34509	Storage Spaces Controller の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-34477	Visual Studio Code .NET Runtime の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34528	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-2021-34529	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-2021-34449	Win32k の特権昇格の脆弱性	重要	7	いいえ	いいえ	EoP
CVE-2021-34516	Win32k の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34491	Win32k の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-34504	Windows Address Book 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-2021-33785	Windows AF_UNIX Socket Provider のサービス拒否の脆弱性	重要	7.5	いいえ	いいえ	DoS
CVE-2021-34459	Windows AppContainer の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34462	Windows AppX Deployment Extensions の特権昇格の脆弱性	重要	7	いいえ	いいえ	EoP
CVE-2021-33782	Windows Authenticode のなりすましの脆弱性	重要	5.5	いいえ	いいえ	Spoofing
CVE-2021-33784	Windows Cloud Files Mini Filter Driver の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34488	Windows Console Driver の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34461	Windows Container Isolation FS Filter Driver の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-33759	Windows Desktop Bridge の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-33745	Windows DNS Server のサービス拒否の脆弱性	重要	6.5	いいえ	いいえ	DoS
CVE-2021-34442	Windows DNS Server のサービス拒否の脆弱性	重要	7.5	いいえ	いいえ	DoS

CVE-2021-34444	Windows DNS Server のサービス拒否の脆弱性	重要	6.5	いいえ	いいえ	DoS
CVE-2021-34499	Windows DNS Server のサービス拒否の脆弱性	重要	6.5	いいえ	いいえ	DoS
CVE-2021-33746	Windows DNS Server のリモートコード実行の脆弱性	重要	8	いいえ	いいえ	RCE
CVE-2021-33754	Windows DNS Server のリモートコード実行の脆弱性	重要	8	いいえ	いいえ	RCE
CVE-2021-33780	Windows DNS Server 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-2021-34525	Windows DNS Server 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-2021-33749	Windows DNS Snap-in 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-2021-33750	Windows DNS Snap-in 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-2021-33752	Windows DNS Snap-in 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-2021-33756	Windows DNS Snap-in 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-2021-33774	Windows Event Tracing の特権昇格の脆弱性	重要	7	いいえ	いいえ	EoP
CVE-2021-34455	Windows File History Service の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34438	Windows Font Driver Host 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-2021-34498	Windows GDI の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34496	Windows GDI の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-34466	Windows Hello 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-2021-34446	Windows HTML Platform のセキュリティ機能バイパスの脆弱性	重要	8	いいえ	いいえ	SFB
CVE-2021-33755	Windows Hyper-V のサービス拒否の脆弱性	重要	6.3	いいえ	いいえ	DoS
CVE-2021-33758	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-2021-34511	Windows Installer の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-33765	Windows Installer のなりすましの脆弱性	重要	6.2	いいえ	いいえ	Spoofing
CVE-2021-31961	Windows InstallService の特権昇格の脆弱性	重要	6.1	いいえ	いいえ	EoP
CVE-2021-34514	Windows カーネル の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34500	Windows カーネル Memory の情報漏えいの脆弱性	重要	6.3	いいえ	いいえ	Info
CVE-2021-34508	Windows カーネル 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-2021-33764	Windows Key Distribution Center の情報漏えいの脆弱性	重要	5.9	いいえ	いいえ	Info
CVE-2021-33788	Windows LSA のサービス拒否の脆弱性	重要	7.5	いいえ	いいえ	DoS
CVE-2021-33786	Windows LSA のセキュリティ機能バイパスの脆弱性	重要	8.1	いいえ	いいえ	SFB
CVE-2021-34447	Windows MSHTML Platform のリモートコード実行の脆弱性	重要	6.8	いいえ	いいえ	RCE
CVE-2021-34493	Windows Partition Management Driver の特権昇格の脆弱性	重要	6.7	いいえ	いいえ	EoP
CVE-2021-33743	Windows Projected File System の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP

CVE-2021-33761	Windows Remote Access Connection Manager の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-33773	Windows Remote Access Connection Manager の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34445	Windows Remote Access Connection Manager の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-34456	Windows Remote Access Connection Manager の特権昇格の脆弱性	重要	7.8	いいえ	いいえ	EoP
CVE-2021-33763	Windows Remote Access Connection Manager の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-34454	Windows Remote Access Connection Manager の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-34457	Windows Remote Access Connection Manager の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-34507	Windows Remote Assistance の情報漏えいの脆弱性	重要	6.5	いいえ	いいえ	Info
CVE-2021-33744	Windows Secure カーネル Mode のセキュリティ機能バイパスの脆弱性	重要	5.3	いいえ	いいえ	SFB
CVE-2021-33757	Windows Security Account Manager Remote Protocol のセキュリティ機能バイパスの脆弱性	重要	5.3	いいえ	いいえ	SFB
CVE-2021-33783	Windows SMB の情報漏えいの脆弱性	重要	5.5	いいえ	いいえ	Info
CVE-2021-31183	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-2021-33772	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-2021-34490	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-2021-34519	Microsoft SharePoint Server の情報漏えいの脆弱性	警告	5.3	いいえ	いいえ	Info

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