# 2021 年 5 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-2021-31204 | .NET Core および Visual Studio の特権昇格の脆弱性 | 重要 | 7.3 | はい | いいえ | EoP |
| CVE-2021-31200 | 共通ユーティリティ のリモートコード実行の脆弱性 | 重要 | 7.2 | はい | いいえ | RCE |
| CVE-2021-31207 | Microsoft Exchange Server のセキュリティ機能バイパスの脆弱性 | 警告 | 6.6 | はい | いいえ | SFB |
| CVE-2021-31166 | HTTP プロトコルスタック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-2021-28476 | Hyper-V 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-2021-31194 | OLE Automation 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-2021-26419 | Scripting Engine のメモリ破損の脆弱性 | 緊急 | 6.4 | いいえ | いいえ | RCE |
| CVE-2021-28461 | Dynamics Finance and Operations のクロスサイトスクリプティングの脆弱性 | 重要 | 6.1 | いいえ | いいえ | XSS |
| CVE-2021-31936 | Microsoft Accessibility Insights for Web の情報漏えいの脆弱性 | 重要 | 7.4 | いいえ | いいえ | Info |
| CVE-2021-31182 | Microsoft Bluetooth Driver のなりすまし の脆弱性 | 重要 | 7.1 | いいえ | いいえ | Spoofing |
| CVE-2021-31174 | Microsoft Excel の情報漏えいの脆弱性 | 重要 | 5.5 | いいえ | いいえ | Info |
| CVE-2021-31195 | Microsoft Exchange Server のリモートコード実行の脆弱性 | 重要 | 6.5 | いいえ | いいえ | RCE |
| CVE-2021-31198 | Microsoft Exchange Server 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-2021-31209 | Microsoft Exchange Server のなりすまし の脆弱性 | 重要 | 6.5 | いいえ | いいえ | Spoofing |

| | | | | | | |
|---|---|---|---|---|---|---|
| CVE-2021-28455 | Microsoft Jet Red Database Engine および Access Connectivity Engine 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-2021-31180 | Microsoft Office Graphics 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-2021-31178 | Microsoft Office の情報漏えいの脆弱性 | 重要 | 5.5 | いいえ | いいえ | Info |
| CVE-2021-31175 | 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-2021-31176 | 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-2021-31177 | 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-2021-31179 | 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-2021-31171 | Microsoft SharePoint の情報漏えいの脆弱性 | 重要 | 4.1 | いいえ | いいえ | Info |
| CVE-2021-31181 | Microsoft SharePoint 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-2021-31173 | Microsoft SharePoint Server の情報漏えいの脆弱性 | 重要 | 5.3 | いいえ | いいえ | Info |
| CVE-2021-28474 | Microsoft SharePoint 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-2021-26418 | Microsoft SharePoint のなりすまし の脆弱性 | 重要 | 4.6 | いいえ | いいえ | Spoofing |
| CVE-2021-28478 | Microsoft SharePoint のなりすまし の脆弱性 | 重要 | 7.6 | いいえ | いいえ | Spoofing |
| CVE-2021-31172 | Microsoft SharePoint のなりすまし の脆弱性 | 重要 | 7.1 | いいえ | いいえ | Spoofing |
| CVE-2021-31184 | Microsoft Windows Infrared Data Association (IrDA) の情報漏えいの脆弱性 | 重要 | 5.5 | いいえ | いいえ | Info |
| CVE-2021-26422 | Skype for Business and Lync 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-2021-26421 | Skype for Business and Lync のなりすまし の脆弱性 | 重要 | 6.5 | いいえ | いいえ | Spoofing |
| CVE-2021-31214 | 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-2021-31211 | Visual Studio Code Remote Development 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-2021-31213 | Visual Studio Code Remote Development 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-2021-27068 | Visual Studio 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-2021-28465 | Web Media 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-2021-31190 | 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-2021-31165 | Windows Container Manager Service の特権昇格の脆弱性 | 重要 | 7.8 | いいえ | いいえ | EoP |
| CVE-2021-31167 | Windows Container Manager Service の特権昇格の脆弱性 | 重要 | 7.8 | いいえ | いいえ | EoP |
| CVE-2021-31168 | Windows Container Manager Service の特権昇格の脆弱性 | 重要 | 7.8 | いいえ | いいえ | EoP |
| CVE-2021-31169 | Windows Container Manager Service の特権昇格の脆弱性 | 重要 | 7.8 | いいえ | いいえ | EoP |
| CVE-2021-31208 | Windows Container Manager Service の特権昇格の脆弱性 | 重要 | 7.8 | いいえ | いいえ | EoP |
| CVE-2021-28479 | Windows CSC Service の情報漏えいの脆弱性 | 重要 | 5.5 | いいえ | いいえ | Info |
| CVE-2021-31185 | Windows Desktop Bridge のサービス拒否の脆弱性 | 重要 | 5.5 | いいえ | いいえ | DoS |
| CVE-2021-31170 | Windows Graphics Component の特権昇格の脆弱性 | 重要 | 7.8 | いいえ | いいえ | EoP |
| CVE-2021-31188 | Windows Graphics Component の特権昇格の脆弱性 | 重要 | 7.8 | いいえ | いいえ | EoP |

| | | | | | | |
|---|---|---|---|---|---|---|
| CVE-2021-31192 | Windows Media Foundation Core 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-2021-31191 | Windows Projected File System FS Filter Driver の情報漏えいの脆弱性 | 重要 | 5.5 | いいえ | いいえ | Info |
| CVE-2021-31186 | Windows Remote Desktop Protocol (RDP) の情報漏えいの脆弱性 | 重要 | 7.4 | いいえ | いいえ | Info |
| CVE-2021-31205 | Windows SMB Client 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-2021-31193 | Windows SSDP Service の特権昇格の脆弱性 | 重要 | 7.8 | いいえ | いいえ | EoP |
| CVE-2021-31187 | Windows Wallet Service の特権昇格の脆弱性 | 重要 | 7.8 | いいえ | いいえ | EoP |
| CVE-2020-24587 | Windows ワイヤレスネットワークの情報漏えいの脆弱性 | 重要 | 6.5 | いいえ | いいえ | Info |
| CVE-2020-24588 | Windows ワイヤレスネットワークのなりすまし の脆弱性 | 重要 | 6.5 | いいえ | いいえ | Spoofing |
| CVE-2020-26144 | Windows ワイヤレスネットワークのなりすまし の脆弱性 | 重要 | 6.5 | いいえ | いいえ | Spoofing |

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