Microsoft 社より 2021 年 9 月のセキュリティ更新プログラムが公開

中国地域サイバーセキュリティ連絡会会員様
中国地域のサイバーセキュリティ担当者様

中国地域サイバーセキュリティ連絡会　事務局の木坂です。

Microsoft 社より 2021 年 9 月のセキュリティ更新プログラムが公開されましたので、以下のとおり情報展開させていただきます。

－－
Microsoft 社により「Critical」と評価される問題を 3 件含むセキュリティ上の問題を修正したプログラムが公開。
早めの対応を推奨。
－－--------

Ⅰ. 概要
　Microsoft 社より 2021 年 9 月度の定例セキュリティアップデートが公開されました。
　対象製品は OS 等の業務利用製品の他、複数のサーバソフトウェア等が対象に含まれます。
　早めのアップデートを推奨します。
　また、すでに悪用が確認されている脆弱性 1 件もアップデートが公開されています。

■対象製品一覧
[OS]
　Windows 7 SP1
　Windows 8.1、RT 8.1
　Windows 10
　Windows 10 Version 1607、1809、1909、2004、20H2、21H1
　Windows Server 2008 SP2、2008 R2 SP1、2012、2012 R2、2016、2019、2022
　Windows Server, version 2004、20H2

[サーバソフトウェア]
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Office Online Server
Azure Open Management Infrastructure

[アプリケーション]
Microsoft 365 Apps for Enterprise
Microsoft Office 2019
Microsoft Office 2016
Microsoft Office 2013 Service Pack 1
Microsoft Office 2013 RT Service Pack 1
Microsoft Visual Studio 2017
Microsoft Visual Studio 2019
MPEG-2 Video Extension
HEVC Video Extensions

Ⅱ. 対策・回避策
影響を受ける製品を利用している場合や、利用しているか不明な場合は、
下記の関連トピックの内容をシステムを運用されている担当者や委託先事業者の窓口の方に共有していただき、
対策等のご検討をお願いいたします。

－－

【関連トピック】
Microsoft 社より 2021 年 9 月のセキュリティ更新プログラムが公開

Windows スクリプトエンジンにおけるメモリ破損の脆弱性や
Windows WLAN AutoConfig サービスの RCE 脆弱性等、Critical 3 件、Important 57 件。
早めの対応を推奨。

－－

Ⅰ. 概要
　Microsoft 社より 2021 年 9 月のセキュリティ更新プログラムが公開されました。
　ベンダー評価 Critical の脆弱性が 3 件(CVE-2021-26435、CVE-2021-36965、CVE-2021-38647)、
Important の脆弱性が 57 件となります。
　また、すでに悪用が確認されているブラウザレンダリングエンジン「MSHTML」の脆弱性「CVE-2021-40444」も
アップデートが公開されています（Ⅲ. 参考情報③)。

■対象製品一覧
※重要度の高い CVSS 7.0 以上の脆弱性が影響する製品を記載しています。
[OS]
　Windows 7 SP1
　Windows 8.1、RT 8.1
　Windows 10
　Windows 10 Version 1607、1809、1909、2004、20H2、21H1
　Windows Server 2008 SP2、2008 R2 SP1、2012、2012 R2、2016、2019、2022
　Windows Server, version 2004、20H2

[サーバソフトウェア]
　Microsoft SharePoint Foundation 2013 Service Pack 1
　Microsoft SharePoint Enterprise Server 2016 Service Pack 1
　Microsoft SharePoint Server 2019
　Microsoft Office Web Apps Server 2013 Service Pack 1
　Microsoft Office Online Server
　Azure Open Management Infrastructure

[アプリケーション]
　Microsoft 365 Apps for Enterprise
　Microsoft Office 2019
　Microsoft Office 2016

Microsoft Office 2013 Service Pack 1
Microsoft Office 2013 RT Service Pack 1
Microsoft Visual Studio 2017
Microsoft Visual Studio 2019
MPEG-2 Video Extension
HEVC Video Extensions

■CVE 番号（CVSS v3.0 基本値）及び概要

※リリースノート（参考情報①）に掲載された CVE 番号のうち、重要度の高い CVSS 7.0 以上を記載しています。

詳細については、Microsoft 社のリリースノート（参考情報①②）を参照ください。

・CVE-2021-26434(7.8)　Visual Studio の特権昇格の脆弱性
・CVE-2021-26435(8.1)　Windows スクリプトエンジンのメモリ破損の脆弱性
・CVE-2021-36952(7.8)　Visual Studio の RCE 脆弱性
・CVE-2021-36954(8.8)　Windows Bind Filter ドライバーの特権昇格の脆弱性
・CVE-2021-36955(7.8)　Windows 共通ログファイルシステムドライバーの特権昇格の脆弱性
・CVE-2021-36960(7.5)　Windows SMB の情報漏えいの脆弱性
・CVE-2021-36963(7.8)　Windows 共通ログファイル システムドライバーの特権昇格の脆弱性
・CVE-2021-36964(7.8)　Windows Event Tracing の特権昇格の脆弱性
・CVE-2021-36965(8.8)　Windows WLAN AutoConfig サービスの RCE 脆弱性
・CVE-2021-36966(7.8)　Windows Subsystem for Linux の特権昇格の脆弱性
・CVE-2021-36967(8.0)　Windows WLAN AutoConfig サービスの特権昇格の脆弱性
・CVE-2021-36968(7.8)　Windows DNS の特権昇格の脆弱性
・CVE-2021-36973(7.8)　Windows リダイレクト ドライブバッファリングシステムの特権昇格の脆弱性
・CVE-2021-36974(7.8)　Windows SMB の特権昇格の脆弱性
・CVE-2021-36975(7.8)　Win32k の特権昇格の脆弱性
・CVE-2021-38625(7.8)　Windows カーネルの特権昇格の脆弱性
・CVE-2021-38626(7.8)　Windows カーネルの特権昇格の脆弱性

・CVE-2021-38628(7.8)　WinSock 用 Windows Ancillary Function Driver の特権昇格の脆弱性
・CVE-2021-38630(7.8)　Windows Event Tracing の特権昇格の脆弱性
・CVE-2021-38633(7.8)　Windows 共通ログファイルシステムドライバーの特権昇格の脆弱性
・CVE-2021-38634(7.1)　Microsoft Windows Update クライアントの特権昇格の脆弱性
・CVE-2021-38638(7.8)　WinSock 用 Windows Ancillary Function Driver の特権昇格の脆弱性
・CVE-2021-38639(7.8)　Win32k の特権昇格の脆弱性
・CVE-2021-38644(7.8)　Microsoft MPEG-2 ビデオ拡張機能の RCE 脆弱性
・CVE-2021-38645(7.8)　Open Management Infrastructure の特権昇格の脆弱性
・CVE-2021-38646(7.8)　Microsoft Office Access Connectivity Engine の RCE 脆弱性
・CVE-2021-38647(9.8)　Open Management Infrastructure の RCE 脆弱性
・CVE-2021-38648(7.8)　Open Management Infrastructure の特権昇格の脆弱性
・CVE-2021-38649(7.0)　Open Management Infrastructure の特権昇格の脆弱性
・CVE-2021-38650(7.6)　Microsoft Office のなりすましの脆弱性
・CVE-2021-38651(7.6)　Microsoft SharePoint Server のなりすましの脆弱性
・CVE-2021-38652(7.6)　Microsoft SharePoint Server のなりすましの脆弱性
・CVE-2021-38653(7.8)　Microsoft Office Visio の RCE 脆弱性
・CVE-2021-38654(7.8)　Microsoft Office Visio の RCE 脆弱性
・CVE-2021-38655(7.8)　Microsoft Excel の RCE 脆弱性
・CVE-2021-38656(7.8)　Microsoft Word の RCE 脆弱性
・CVE-2021-38658(7.8)　Microsoft Office Graphics の RCE 脆弱性
・CVE-2021-38659(7.8)　Microsoft Office のリモートコードが実行される脆弱性
・CVE-2021-38660(7.8)　Microsoft Office Graphics の RCE 脆弱性
・CVE-2021-38661(7.8)　HEVC ビデオ拡張機能の RCE 脆弱性
・CVE-2021-38667(7.8)　Windows 印刷スプーラーの特権昇格の脆弱性
・CVE-2021-38671(7.8)　Windows 印刷スプーラーの特権昇格の脆弱性
・CVE-2021-40447(7.8)　Windows 印刷スプーラーの特権昇格の脆弱性

Ⅱ. 対策・回避策

以下のベンダ情報（Ⅲ. 参考情報）をもとに、更新プログラムの適用を検討ください。

また、すぐに更新プログラムを適用できない場合は回避策の適用も併せてご検討ください。

Ⅲ. 参考情報

① 2021 年 9 月のセキュリティ更新プログラム
https://msrc.microsoft.com/update-guide/releaseNote/2021-Sep

② セキュリティ更新プログラムガイド
https://portal.msrc.microsoft.com/ja-jp/security-guidance

③ 9/15 更新(プロ)【重要】MS Windows に含まれるブラウザのレンダリングエンジン「MSHTML」にゼロデイ脆弱性

https://www.csircc.go.jp/sns/sns/index.php?command=getarticle&asid=2134000&aid=40186002001