【修正】 Microsoft Windows OS に深刻なセキュリティ上の問題

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。

先日、下記メールにより情報展開させていただきました、
Microsoft Windows OS の深刻なセキュリティ上の問題に関して
【関連トピック】の修正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。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【関連トピック】
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

Microsoft 社より、ブラウザのレンダリングエンジン「MSHTML」のゼロデイ脆弱性が公開。
対策、回避策、緩和策が公開されているため、早急な対応を推奨。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

Ⅰ. 概要
　Microsoft 社はレンダリングエンジン「MSHTML」のゼロデイ脆弱性を公開しました。
　ActiveX コントロールが埋め込まれた悪意のある Microsoft Office ドキュメントをブラウザで開いた場合に、
リモートからコードを実行される可能性があります。
　※本脆弱性を悪用する標的型攻撃がベンダにより確認されています。

影響：
　この脆弱性を悪用された場合、機密情報の奪取、任意のコマンド実行、機器の乗っ

取りに悪用される恐れがあります。

■対象製品一覧
・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
・Windows Server Version 2004、2008、2012、2016、2019、2022、20H2
※最新の情報や詳細なバージョン等は参考情報①をご参照ください。

■概要及び CVE 番号（CVSS v3.0 基本値）
・レンダリングエンジン「MSHTML」 のリモートでコードが実行される脆弱性
・CVE-2021-40444(8.8)

Ⅱ. 対策・回避策
〇対策
現時点で本脆弱性に対する Windows OS のアップデートは提供されておりませんが、
マルウェア対策「Microsoft Defender Antivirus(Windows 10 に標準で付属)」または「Microsoft Defender for Endpoint」をご利用の場合、検出ビルド 1.349.22.0 以降で同脆弱性に対する攻撃の検知および保護に対応していますので、
ご確認の上必要に応じてビルドのアップデートをお願いします。

[緩和策]
次の緩和策の適用をご検討ください。
・インターネット上のドキュメントは「Protected View」または「ApplicationGuard for Office」で開く。
※信頼できない Microsoft Office ドキュメントは開かないようご注意ください。

[回避策]
Microsoft 社から公開された回避策には、次のような設定による影響回避について記載されています。
・グループポリシーまたは regkey を介して ActiveX コントロールのインストールを無効にする。

・Windows エクスプローラーでプレビューを無効にする。

※レジストリエディタを誤って使用すると、オペレーティングシステムの再インストールが必要になる
場合もございますので、十分ご注意の上ご対応ください。

Ⅲ. 参考情報
①Microsoft MSHTML Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
②Microsoft Releases Mitigations and Workarounds for CVE-2021-40444
https://us-cert.cisa.gov/ncas/current-activity/2021/09/07/microsoft-releases-mitigations-and-workarounds-cve-2021-40444

以上です。
よろしくお願いします。

-----Original Message-----
From: ｃｈｕｃｙｂｅｒ
Sent: Wednesday, September 8, 2021 5:15 PM
To: ｃｈｕｃｙｂｅｒ <chucyber@soumu.go.jp>
Subject: Microsoft Windows OS に深刻なセキュリティ上の問題【中国地域サイバーセキュリティ連絡会】

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 Windows OS に深刻なセキュリティ上の問題について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。
－－－

機器の乗っ取りにつながる恐れのある問題。

既に悪用されている事が確認されているため、早急に対応することを推奨します。
－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

Ⅰ．概要
　Windows OS で HTML（Web ページの記述用言語）で書かれた文書を解釈し、
記述された文書や画像などを描画するためのプログラム「MSHTML」に、
機器の乗っ取りに繋がる恐れのある問題が存在し、Microsoft 社より定例外で
セキュリティの問題に関する情報が公開されました。
　既に悪用されていることが確認されているため、早急に対策することを強く推奨します。

■対象製品一覧
　・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
　・Windows Server Version 2004、2008、2012、2016、2019、2022、20H2

Ⅱ．対策・回避策
　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、回避策、または緩和策の適用を検討してください。
－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【関連トピック】
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

Microsoft 社より、ブラウザのレンダリングエンジン「MSHTML」のゼロデイ脆弱性が公開。
対策、回避策、緩和策が公開されているため、早急な対応を推奨。

－－

Ⅰ．概要

　Microsoft 社はレンダリングエンジン「MSHTML」のゼロデイ脆弱性を公開しました。

　ActiveX コントロールが埋め込まれた悪意のある Microsoft Office ドキュメントをブラウザで開いた場合に、リモートからコードを実行される可能性があります。

　※本脆弱性を悪用する標的型攻撃がベンダにより確認されています。

影響：この脆弱性を悪用された場合、機密情報の奪取、任意のコマンド実行、
　　機器の乗っ取りに悪用される恐れがあります。

■対象製品一覧

- 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
- Windows Server Version 2004、2008、2012、2016、2019、2022、20H2

■概要及び CVE 番号（CVSS v3.0 基本値）

・レンダリングエンジン「MSHTML」 のリモートでコードが実行される脆弱性
　・CVE-2021-40444(8.8)

Ⅱ．対策・回避策

〇対策

　現時点で本脆弱性に対する Windows OS のアップデートは提供されておりませんが、
マルウェア対策「Microsoft Defender Antivirus(Windows 10 に標準で付属)」または「Microsoft Defender for Endpoint」をご利用の場合、検出ビルド 1.349.22.0 以降で同脆弱性に対する攻撃の検知および保護に対応していますので、ご確認の上
必要に応じてビルドのアップデートをお願いします。

〇回避策

次の回避策の適用をご検討ください。

・インターネット上のドキュメントは「Protected View」または「ApplicationGuard for Office」で開く。

〇一時的な緩和策

Microsoft 社から公開された緩和策には、次のような設定による影響回避について記載されています。

・Internet Explorer ですべての ActiveX コントロールのインストールを無効にする。

※ActiveX コントロールのインストール無効化にはレジストリの更新が必要となり、
レジストリエディタを誤って使用すると、オペレーティングシステムの再インストールが
必要になる場合もございますので、十分ご注意の上ご対応ください。

Ⅲ. 参考情報

①Microsoft MSHTML Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

②Microsoft Releases Mitigations and Workarounds for CVE-2021-40444
https://us-cert.cisa.gov/ncas/current-activity/2021/09/07/microsoft-releases-mitigations-and-workarounds-cve-2021-40444