

2024年5月15日

内閣官房 内閣サイバーセキュリティセンター
重要インフラグループ

マイクロソフト製ソフトウェアの深刻な脆弱性について(注意喚起)

1. 対象ソフトウェア

- ・ Microsoft Windows、Microsoft Office 等の複数のマイクロソフト製ソフトウェア
(対象ソフトウェアの一覧は、参考 URL 参照)

2. 脆弱性悪用による影響等

任意のコードを実行（プログラムの実行、異常終了、当該コンピュータに保存されているデータの改ざん・削除・漏洩等）される恐れがあります。

3. 悪用

脆弱性を悪用した攻撃が確認されています。

4. 対応

本脆弱性の修正を含むセキュリティ更新プログラムを適用してください。

5. その他

セキュリティ更新プログラム（参考 URL①）にて修正された脆弱性のうち、深刻な脆弱性は CVE-2024-30040（参考 URL②）及び CVE-2024-30051（参考 URL③）です。

参考 URL

- ① 2024年5月のセキュリティ更新プログラム（月例）(マイクロソフト)
<https://msrc.microsoft.com/blog/2024/05/202405-security-update/>
- ② Windows MSHTML プラットフォームのセキュリティ機能のバイパスの脆弱性（マイクロソフト）
<https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2024-30040>
- ③ Windows DWM Core ライブラリの特権の昇格の脆弱性(マイクロソフト)
<https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2024-30051>