TLP:CLEAR【全分野】

別紙

2024 年 2 月 14 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
セキュリティ更新プログラムについて(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）される恐れがある脆弱性が含まれます。

3. 深刻度
   ソフトウェアの開発元が深刻度「Critical」(4 段階中、最高)に分類する脆弱性が含まれます。

4. 悪用
   開発元により悪用が確認されている脆弱性が含まれます。

5. 対応
   セキュリティ更新プログラム等を適用してください。

6. その他
   今回修正された脆弱性には、更新プログラムが公開されるよりも前に悪用や脆弱性の詳細が公開され、ゼロデイ攻撃が可能となっていたものが含まれます。特に次の脆弱性については、攻撃者によって細工されたファイルを実行することでマルウェアに感染する可能性があり、悪用が容易であることから、早急にセキュリティ更新プログラムを適用してください。
   - Windows SmartScreen のセキュリティ機能のバイパスの脆弱性(CVE-2024-21351)
   - インターネット ショートカット ファイルのセキュリティ機能のバイパスの脆弱性(CVE-2024-21412)

参考 URL
- 2024 年 2 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/2024/02/202402-security-update/
- Windows SmartScreen 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-2024-21351
- インターネットショートカットファイルのセキュリティ機能(マイクロソフト)
  https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2024-21412