電子成果品作成支援・検査システムにおける任意のDLL読み込みに関する脆弱性の注意喚起

公開日 2017年6月20日

■概要

電子成果品作成支援・検査システムの自己解凍書庫及びインストーラーに、任意のDLL読み込みに関する脆弱性が存在することが判明しました。

この脆弱性を悪用された場合、悪意ある第三者の攻撃により、意図しないDLLを実行してしまう恐れがあります。

■脆弱性の説明

電子成果品作成支援・検査システムは、ファイルの自己解凍のためにLhaplusの機能を搭載しています。自己解凍時、任意のDLLの読み込みにより、カレントディレクトリを含む複数のフォルダを検索してDLLを読み込みますが、カレントディレクトリを優先して検索するため、悪意ある第三者の攻撃により、意図しないDLLを実行してしまう恐れがあります。

■脆弱性がもたらす脅威

管理者権限で任意のコードを実行される可能性があります。

■対策方法

平成29年6月9日以前にダウンロードした本システムファイルを確実に削除してください。

■回避策

この脆弱性は、次に示す手順で影響を緩和できる場合があります。

・自己解凍書庫の実行を新規に作成したフォルダ内で行う。

・本システムのインストーラーの起動を新規に作成したフォルダ内で行う。

■関連情報

JVNDB-2010-000037：Lhaplus における DLL 読み込みに関する脆弱性

■謝辞

橘総合研究所の英利雅美氏よりこの問題をご報告いただきました。