

Microsoft Windows User32.DLL ANI File Header Handling Stack-Based Buffer Overflow Vulnerability

分類 Boundary Condition Error/受動的攻撃

再現性 リモート

技術解説

1)概要

Microsoft Windows に実装されている User32.dll にはバッファオーバーフローが発生する問題が存在する。この問題を悪用した受動的攻撃により、Internet Explorer (以下「IE」という。)などを利用して、問題のある ANI ファイルを参照することで、参照したユーザの権限で任意のコードを実行される可能性がある。

また、この問題は、Microsoft Security Bulletin MS05-002 の一つ、「カーソルおよびアイコンのフォーマットの処理の脆弱性」として公開されている。「カーソルおよびアイコンのフォーマットの処理の脆弱性」には、整数オーバーフローとスタックオーバーフローの二つの脆弱性が存在し、この問題はスタックオーバーフローの問題である。

対策方法

1)対策

Windows Update を利用することにより、マイクロソフト社から提供されている修正プログラム(891711)を適用する。また、Windows Update を利用しない場合は、下記の参考サイトなどを参考にして、個別に修正プログラムを入手し適用する。

Windows Update :

<http://windowsupdate.microsoft.com/>

参考サイト:

<http://www.microsoft.com/japan/technet/security/bulletin/MS05-002.asp>

2)Advisory情報

Microsoft Security Bulletin MS05-002 (英語版):

<http://www.microsoft.com/technet/security/bulletin/ms05-002.msp>

Microsoft Security Bulletin MS05-002 (日本語版):

<http://www.microsoft.com/japan/technet/security/bulletin/MS05-002.asp>

eeye Digital Security :

<http://www.eeye.com/html/research/advisories/AD20050111.html>

SecurityFocus BID 12233:

<http://www.securityfocus.com/bid/12233/>