

UPnP NOTIFY Buffer Overflow Vulnerability

分類 Buffer Overflow
 関連ツール名称
 再現性 リモート

技術解説

1) 概要

Windows OSで実装されている UPnP(Universal Plug and Play)には、リモートから不正な UDP NOTIFY パケットを受信することによって、バッファオーバーフローが発生する問題がある。この問題を利用して、リモートから任意のコマンドを実行することが可能である。

2) 原因

UPnPは、ローカルホスト上のデバイスを対象としたPlug and Playを拡張し、ネットワーク上のデバイスを検知し、そのデバイスの情報を確認できるようにするサービスである。

新しいデバイスがネットワーク上のホストに追加されると、それを知らせるために以下のようなデータを含む udp パケットをマルチキャストアドレスに送信する。(黄色の部分には追加されるデバイスによって異なる。)

```
NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
CACHE-CONTROL: max-age = seconds until advertisement expires
LOCATION: URL for UPnP description for root device
NT: search target
NTS: ssdp:alive
SERVER: OS/version UPnP/1.0 product/version
USN: advertisement UUID
```

UPnPは、LOCATION ヘッダの引数として与えられた文字列をチェックしていないため、LOCATION ヘッダの引数の文字列を徐々に増やしていくと、あるタイミングでバッファオーバーフローが発生する。バッファオーバーフローが発生するタイミングについては明らかにされていない。

UPnP NOTIFY Buffer Overflow Vulnerability

検証有無

結果 ○: 成功、×: 失敗、-: 未検証

OS	サービス	バージョン	結果
Windows XP Professional Edition (J)	Universal Plug and Play		×
上記以外			-

検証結果

1) 検証環境

	OS	サービス	備考
攻撃側	RedHat Linux 7J		
ターゲット	Windows XP Professional Edition(J)	Universal Plug and Play	

2) 検証結果

バッファオーバーフローの発生は確認できなかった。

痕跡

1) ログ

なし

2) 痕跡

なし

影響

Windows OSで実装されているUniversal Plug and Playには、バッファオーバーフローが発生する問題が存在し、リモートから任意のコマンドを実行することが可能である。

影響を受けるOS、サービス

影響 ○:脆弱性あり、×:脆弱性なし

(2001/12/20現在)

OS	サービス	バージョン	影響	備考
Windows	Universal Plug and Play	98	○	デフォルトではインストールされていない
		98SE	○	デフォルトではインストールされていない
		ME	○	
		XP	○	

OS、サービス Windows 98/98SE/ME/XP
アプリケーション Universal Plug and Play

対策方法

1)対策

この問題を修正するhotfixを適用する。

hotfix入手先 URL:

http://www.microsoft.com/japan/technet/security/frame_prekb.asp?sec_cd=MS01-059

2)Advisory情報

Microsoft Security Bulletin MS01-059:

http://www.microsoft.com/japan/technet/security/frame_prekb.asp?sec_cd=MS01-059