

[NT] Microsoft Windows Media Player Plugin Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00055.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2006 13:27:16 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Microsoft Windows Media Player Plugin Buffer Overflow

SUMMARY

" <<http://www.microsoft.com/windows/windowsmedia/mp10/default.aspx>>
Windows Media Player gives you more music and more choices, and for the first time makes it possible to sync high-quality music, video, and photos to the latest portable devices."

Improper handling of user input allows attackers to execute arbitrary code using Microsoft Windows Media Player.

DETAILS

Vulnerable Systems:

- * Windows Media Player version 9
- * Windows Media Player version 10

Windows Media Player (WMP) can be launched as a plugin in popular browsers to view Windows Media Player file types from web pages.

A vulnerability in the Windows Media Player plugin can be triggered from several popular browsers such as FireFox and Netscape. The issue

[NT] Microsoft Windows Media Player Plugin Buffer Overflow

specifically can be triggered when certain browsers launch it with an overly long embed src tag from a malicious html page.

Upon successful exploitation, attackers will be able to overwrite a Structured Exception Handler (SEH) address and execute arbitrary code on the system.

The vulnerability specifically lays in npdsplay.10001040 where a user supplied string is copied to a stack based buffer:

```
1000171A C1E9 02 SHR ECX,2
```

```
1000171D F3:A5 REP MOVS DWORD PTR ES:[EDI],DWORD PTR
```

```
DS:[ESI]
```

```
1000171F 8BC8 MOV ECX,EAX
```

With properly crafted input the attacker is able to execute code of his choice. Due to unicode translations, shellcode characters are somewhat limited to character code values below 0x80. Successful exploitation of this vulnerability is not significantly impacted by this limitation.

Successful exploitation of this vulnerability allows attackers to execute code within the context of the currently logged in user. The victim would have to visit a malicious website using Firefox, Netscape browsers for example and have Windows Media Player installed.

Workaround:

Associate media files with different media player than Microsoft Windows Media Player.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0005>>
CVE-2006-0005

Disclosure Timeline:

08/31/2005 Initial vendor notification

08/31/2005 Initial vendor response

02/14/2006 Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@xxxxxxxxxxxxxxxxxxxxx>> iDEFENSE Labs.

The original article can be found at:

<<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=393>>

<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=393>

The vendor advisory can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS06-006.msp>>

<http://www.microsoft.com/technet/security/bulletin/MS06-006.msp>

[NT] Microsoft Windows Media Player Plugin Buffer Overflow

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.