

## TopResponse Threat Advisory

**Release Date:** April 4, 2007

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks against the Microsoft Windows Animated Cursor ANI File Overflow (CVE-2007-0038).

**Top Layer Products:** IPS 5500 Version 3.40 and higher.

**Vulnerable Infrastructure:** Microsoft Windows NT, Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista.

**Alert Type:** Targeted protection

**Risk Assessment:** Critical

**Threat Impact:** Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems.

**Advisory Impact:** Prevention

**Summary:** The Microsoft Windows Animated Cursor (ANI) File Overflow vulnerability could allow an attacker to execute arbitrary code on the user's system in the security context of the logged-on user by enticing the user to visit a specially crafted web page or open a specially crafted file.

**Recommended Action:** Top Layer recommends the following actions:

TopResponse™ Users: Download and apply Protection Pack 2007-04-03-03 (or later) to put this new protection into place. This is automatically applied to the "recommended" client protection ruleset. Make sure you created and applied the HTTP-Client string set, as described in the TopResponse WMF Advisory from December 29, 2005.

### **IPS 5500 Manual Configuration Instructions:**

Note: There are different instructions for IPS 5500 Version 3.40 and Version 4.X.

### Instructions for Version 3.40:

Version 3.40 users should complete the following steps:

1. Log into the Web Management Interface of your IPS 5500.
2. Select **IPS Configuration->Filter Configuration->Payload Signatures->Patterns**.
3. Click the **Add** button.
4. Enter the following for the new entry:

Note: If you have not created the HTTP-Client string set yet, as described in the TopResponse WMF Advisory from December 29, 2005, you should do so before proceeding.

Signature:

|61 6E 69 68 A8 01 00 00 0B 0B 0B 0B 0B 0B 0B|

String Set:

HTTP-Client

ID Label:

040307.ANL1

5. Click the **Done** button.
6. Click the **Add** button.
7. Enter the following for the new entry:

Signature:

|61 6E 69 68 FF FF 00 00 0D 0D 0D 0D 0D 0D 0D|

String Set:

HTTP-Client

ID Label:

040307.ANL2

8. Click the **Done** button.
9. Click the **Add** button.
10. Enter the following for the new entry:

Signature:

|61 6E 69 68 A8 01 00 00 08 08 08 08 08 08 08|

String Set:

HTTP-Client

ID Label:

040307.ANL3

11. Click the **Done** button.
12. Click the **Close** button.
13. Click the **Apply** button.
14. Click the **Save** button.

**Instructions for Version 4.X:**

Version 4.X users should complete the following steps:

1. Log into the Web Management Interface of your IPS 5500.
2. Select **Configure Security->Advanced Security Config->IPS Rules Customization-> ->Attack Signatures->Patterns.**
3. Click the **Add** button.
4. Enter the following for the new entry:

**Note:** *If you have not created the HTTP-Client string set yet, as described in the TopResponse WMF Advisory from December 29, 2005, you should do so before proceeding.*

Signature:

|61 6E 69 68 A8 01 00 00 0B 0B 0B 0B 0B 0B 0B|

String Set:

HTTP-Client

ID Label:

040307.ANL1

5. Click the **Done** button.
6. Click the **Add** button.
7. Enter the following for the new entry:

**Note:** *If you have not created the HTTP-Client string set yet, as described in the TopResponse WMF Advisory from December 29, 2005, you should do so before proceeding.*

Signature:

|61 6E 69 68 FF FF 00 00 0D 0D 0D 0D 0D 0D 0D|

String Set:

HTTP-Client

ID Label:

040307.ANL2

8. Click the **Done** button.
9. Click the **Add** button.
10. Enter the following for the new entry:

**Note:** *If you have not created the HTTP-Client string set yet, as described in the TopResponse WMF Advisory from December 29, 2005, you should do so before proceeding.*

Signature:

|61 6E 69 68 A8 01 00 00 08 08 08 08 08 08 08|

String Set:

HTTP-Client

ID Label:

040307.ANL3

11. Click the **Done** button.
12. Click the **Apply** button.
13. Click the **Close** button.
14. Click the **Save** icon (upper left of your GUI).

**References:** Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
Microsoft Security Advisory	<a href="http://www.microsoft.com/technet/security/advisory/935423.mspix">http://www.microsoft.com/technet/security/advisory/935423.mspix</a>
Microsoft Security Bulletin	<a href="http://www.microsoft.com/technet/security/bulletin/ms07-017.mspix">http://www.microsoft.com/technet/security/bulletin/ms07-017.mspix</a>

**Relevant TLN Rules:** tln-106142

**Relevant TopResponse Protection Pack(s):** 2007-04-03-03