

TopResponse Threat Advisory

Release Date: July 28, 2006

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block an exploit for the Microsoft DHCP Buffer Overflow (CVE-2006-2372, MS06-036) Vulnerability.

Top Layer Products: IPS 5500 Version 3.40 and higher.

Vulnerable Infrastructure: Microsoft Windows 2000 SP4, Windows XP SP1 and SP2, and Server 2003 up to SP1.

Alert Type: Targeted protection

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems using a publicly available exploit.

Advisory Impact: Prevention

Summary: The Microsoft DHCP Buffer Overflow vulnerability could allow a remote attacker to execute arbitrary code on the targeted system via a crafted DHCP response.

Recommended Action: Top Layer recommends the following actions:

TopResponse Update Manager™ Users: Download and apply Protection Pack 2006-07-28-04 (or later) and follow the instructions in the Protection Pack notes to put this new protection into place.

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->Sets**
3. Select the next available unused "User-*nn*", and click the **Edit** button.
4. Change the name to "DHCP-Client"
5. Select **Patterns**
6. Click the **Add** button.

7. Enter the following for the new entry:

Signature:

|31 c9 83 e9 cb d9 ee d9 74 24 f4 5b 81 73 13 13|

String Set:

DHCP-Client

ID Label:

060723.1

8. Click the **Done** button.
9. Click the **Close** button.
10. Select **IPS Configuration->Groups and Services->Services**
11. Select **bootpCInt/udp68** and click the **Edit** button.
12. Click the **Advanced** button, and set **Process-As** to **PAYLOAD-PATTERN-SEARCH**.
13. Set **Client to Server Stringset** to **DHCP-Client**.
14. Click **OK, OK, Close**.
15. Click the **Apply** button, and 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->Sets**
3. Select the next available unused "User-nn", and click the **Edit** button.
4. Change the name to "DHCP-Client"
5. Select **Patterns**
6. Click the **Add** button.
7. Enter the following for the new entry:

Signature:

|31 c9 83 e9 cb d9 ee d9 74 24 f4 5b 81 73 13 13|

String Set:

DHCP-Client

ID Label:

060723.1

8. Click the **Done** button.
9. Click the **Close** button.
10. Select **Configure Security->Security Policies**
11. Select the **Services tab**
12. Select **bootpCInt/udp68** and click the **Edit** button.
13. Click the **Advanced** button, and set **Process-As** to **PAYLOAD-PATTERN-SEARCH**.

14. Set **Client to Server Stringset** to **DHCP-Client**.
15. Click the **OK** button, and the next **OK** button.
16. 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	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS06-036.msp

Relevant TLN Rules: TLN-106134

Relevant TopResponse Protection Pack(s): 2006-07-28-04