

TopResponse Threat Advisory

Release Date: June 12, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory which provides information needed to provide protection for the following:

Microsoft Visual Studio MSCOMM32.OCX Buffer Overflow ActiveX Vulnerability (CVE-2008-0024)

HP Virtual Rooms Client ActiveX Vulnerability (CVE-2009-0208)

eBay Enhanced Picture Uploader ActiveX Vulnerability (CVE-2008-2475)

Microgaming FlashAX ActiveX Vulnerability (CVE-2008-5691)

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure:

Microsoft Windows 2000 SP4, Windows XP SP2 and Windows SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 x64 Edition SP2, and Windows Server 2003 with SP2 for Itanium-based Systems, Windows Vista, Windows Vista SP1 and SP2, Windows Vista x64 Edition, Windows Vista x64 Edition SP1 and SP2, Microsoft Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems SP2, and Windows Server 2008 for x64-based Systems, as well as Windows Server 2008 for x64-based Systems SP2;

HP Virtual Rooms Client v7.0.1 and earlier running on Windows;

eBay Enhanced Picture Uploader ActiveX Control prior to January 2009 in the following flows and products:

- eBay.com: Sell Your Item (SYI), Setup & Test eBay Enhanced Picture Services, Picture Manager Enhanced Uploader
- CARad.com: Add Vehicle

Microgaming FlashAX ActiveX Control for all versions prior to and including 1.0.1.8.

Alert Type: Critical Vulnerabilities

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerabilities that could allow an attacker to control vulnerable systems

Advisory Impact: Prevention

Summary:

Each of the vulnerable ActiveX controls has reported vulnerabilities that could allow an attacker to execute arbitrary code on the client system in the context of the logged-on user by enticing the user to open a specially crafted web page.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-06-12-02 (or later) to put this new protection into place. Protection for these vulnerabilities is automatically applied to the IPS Rule Sets detailed in the table below.

In order to take advantage of the protection, make sure the IPS rules are enabled in the IPS Rule Set used to inspect traffic to your client infrastructure.

Rule ID	CVE ID	Description	Client	Server
tln-106252	CVE-2008-0024	Microsoft Visual Studio MSCOMM32.OCX Buffer Overflow	Recommended	--
tln-106251	CVE-2009-0208	HP Virtual Rooms Client	Recommended	--
tln-106250	CVE-2008-2475	eBay Enhanced Picture Uploader	Strict	--
tln-106249	CVE-2008-5691	Microgaming FlashAX	Recommended	--

Note: The IPS rule tln-106250 is currently enabled in the Strict IPS Rule Sets because there is a potential for false positive events. Please monitor events after the rule is enabled to provide protection for this vulnerability.

To manually enable this rule in any IPS Rule Set complete the following steps:

1. Log into the Web Management Interface of your IPS 5500 E-Series.
 2. Select **Configure Security->Security Policies**.
 3. Select the **IPS Rule Sets** tab.
 4. Select the Rule Set for which you want to change the setting of rule tln-106250.
 5. Enter **106250** in the search window.
 6. Double click on the rule **tln-106250 EXPLT: eBay Enhanced Picture Uploader ActiveX Vulnerability**.
 7. Make sure that the **Enabled** button is checked.
 8. Make sure that the **Action** is set to **DROP**.
 9. Click the **OK** button.
- Repeat steps 4 through 9 for all other Rule Sets that you want to change.
10. Close the Configure Security Policies window.
 11. Click the **Save** icon (upper left of your GUI).

References: Use the following sources for additional information:

Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/advisory/969898.mspx
eBay Advisory	http://pages.ebay.com/securitycenter/activex/index.html
HP Advisory	http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01678405
Microgaming Advisory	http://www.microgaming.co.uk/news_flashxcontrol.php
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0024 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5691 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2475 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0208

Relevant TLN Rules: tln-106249, tln-106250, tln-106251 and tln-106252

Relevant TopResponse Protection Pack(s): 2009-06-12-02