

TopResponse Threat Advisory

Release Date: February 10, 2009

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

Microsoft Internet Explorer v7 CSS Remote Code Execution Vulnerability (MS09-002, CVE-2009-0076)

Known Attack against a Microsoft Internet Explorer v7 Clickjacking Vulnerability (No CVE currently assigned)

Opera Browser File URI Handling Vulnerability (CVE-2008-5178)

HP Instant Support HPISDataManager ExtractCab Vulnerability (CVE-2008-0952)

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure:

Internet Explorer v7 on Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3, Microsoft Windows XP Professional x64 Edition, Microsoft Windows XP Professional x64 Edition Service Pack 2, Microsoft Windows Server 2003 Service Pack 1, Microsoft Windows Server 2003 Service Pack 2, Microsoft Windows Server 2003 x64 Edition, Microsoft Windows Server 2003 x64 Edition Service Pack 2, Microsoft Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft Windows Vista and Windows Vista Service Pack 1, Microsoft Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1, Microsoft Windows Server 2008 for 32-bit Systems, Microsoft Windows Server 2008 for x64-based Systems, Microsoft Windows Server 2008 for Itanium-based Systems;

HP Instant Support HPISDataManager ExtractCab ActiveX control for Microsoft Windows – versions prior to 1.0.0.24;

Opera web browser – versions prior to 9.62.

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:

Microsoft Internet Explorer v7 is a common web browser used by Microsoft client infrastructure to retrieve and render content from the network. The reported vulnerability targets a cross-site scripting weakness that will coerce Microsoft Internet Explorer v7 into handling memory of an object that has previously been deleted. The vulnerability could allow a remote 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.

Clickjacking is a method of obfuscating malicious code within the client browser. The user is enticed to activate code from a page on a web site that they believe to be safe. Protection for a known attack against Microsoft Internet Explorer v7 is provided.

The Opera web browser and Internet suite is a free application for personal computer users to perform common tasks on the Internet. The buffer overflow vulnerability was discovered in Opera versions before v9.62. This vulnerability allows remote attackers to execute arbitrary code on the client system as the result of parsing an overly long URI. The exploited Uniform Resource Identifier (URI) will contain the prefix format of "file://path/file". The reported vulnerability could allow an attacker to execute arbitrary code on the user's system in the context of the logged-on user by enticing the user to open a specially crafted web page. The protection previously provided by the IPS E-Series has been enhanced.

The HPISDataManagerLib.Datamgr ActiveX control in HPISDataManager.dll in HP Instant Support before 1.0.0.24 allows remote attackers to create files with arbitrary content on the client system. The ExtractCab function is vulnerable to exploitation.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-02-10-03 (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-106226	CVE-2009-0076	Microsoft Internet Explorer v7 CSS Remote Code Execution	Strict	--
tln-106225	No CVE Number	Microsoft Internet Explorer v7 Clickjacking	Recommended	Recommended
tln-106140	CVE-2008-5178	Opera Browser File URI Handling	Recommended	--
tln-106224	CVE-2008-0952	HP Instant Support ExtractCab	Recommended	Recommended

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 106226
 5. Enter **106226** in the search window
 6. Double click on the rule **tln-106226 EXPLT: Microsoft Internet Explorer v7 CSS Remote Code Execution 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:

Additional Information	Location
Top Layer Support Web site	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/MS09-002.msp
Milw0rm Advisory	URL:http://www.milw0rm.com/exploits/7912
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0076 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5178 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0952

Relevant TLN Rules: tln-106140, tln-106224, tln-106225 and tln-106226