

TopResponse Threat Advisory

Release Date: February 13, 2009

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

Microsoft SQL Server sp_replwritetovarbin Vulnerability
(MS09-004, CVE-2008-5416)

Microsoft Internet Explorer v7 Uninitialized Memory Corruption
Vulnerability (MS09-002, CVE-2009-0075)

Microsoft Visual Basic ActiveX Controls Animation Object Vulnerability
(MS08-070, CVE-2008-4255)

RIM Blackberry Application Web Loader ActiveX Control Buffer
Overflow (CVE-2009-0305)

Akamai Download Manager File Download to Arbitrary Location
Vulnerability (CVE-2008-1770)

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure:

Microsoft SQL Server 2000 SP4, Microsoft SQL Server 2000 Itanium-based Edition SP4, Microsoft SQL Server 2005 SP2, Microsoft SQL Server 2005 x64 Edition SP2, Microsoft SQL Server 2005 with SP2 for Itanium-based Systems, Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) SP4, Microsoft SQL Server 2005 Express Edition SP2, Microsoft SQL Server 2005 Express Edition with Advanced Services SP2.

Internet Explorer v7 on Microsoft Windows XP SP2, Microsoft Windows XP SP3, Microsoft Windows XP Professional x64 Edition, Microsoft Windows XP Professional x64 Edition SP2, Microsoft Windows Server 2003 SP1, Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2003 x64 Edition, Microsoft Windows Server 2003 x64 Edition SP2, 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 SP1, Microsoft Windows Vista x64 Edition and Windows Vista x64 Edition SP1, Microsoft Windows Server 2008 for 32-bit Systems, Microsoft Windows Server 2008 for x64-based Systems, Microsoft Windows Server 2008 for Itanium-based Systems;

Microsoft Visual Basic 6.0 Runtime Extended Files; Microsoft Visual Studio .NET 2002 SP1; Microsoft Visual Studio .NET 2003 SP1; Microsoft Visual FoxPro 8.0 SP1; Microsoft Visual FoxPro 9.0 SP1; Microsoft Visual FoxPro 9.0 SP2; Microsoft Office FrontPage 2002 SP3; Microsoft Office Project 2003 SP3; Microsoft Office Project 2007 SP1

RIM BlackBerry Application Web Loader ActiveX control (AxLoader)
version 1.0

Akamai Download Manager ActiveX Control versions prior to 2.2.3.5.

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 SQL Server is a relational database management system (RDBMS). The reported vulnerability is where a parameter is not properly validated in one of the extended stored procedures, "sp_replwritetovarbin". Typically, remote exploitation requires authenticated access to the database so an authenticated user can call the stored procedure "sp_replwritetovarbin". If the attacker can leverage a SQL injection vulnerability, they can possibly exploit this vulnerability without authentication.

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 how 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.

Components from Visual Basic 6 are utilized and redistributed with products built using this development environment. The various ActiveX Controls for Visual Basic 6 are also available in other development environments, such as Microsoft .Net and Microsoft FoxPro. The reported vulnerabilities target the Microsoft ActiveX Animation Object control. The vulnerability 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. IPS rule tln-106218 has been enhanced to provide additional protection.

The Akamai Download Manager is an application that allows the user to manage the download of content. The reported vulnerability enables the attacker to write their file to an arbitrary location on the client system. The vulnerability is exploited when the user is enticed to visit a malicious URL. It is possible the unauthorized download can be followed by execution of arbitrary code in the context of the logged in user.

The BlackBerry Application Web Loader is a Microsoft ActiveX control that is used by third party application developers to install applications directly on a BlackBerry mobile device. The BlackBerry mobile device is connected by USB to the Windows client system before the vulnerable Web Loader ActiveX control is activated. The vulnerability could allow an attacker to execute arbitrary code on the Windows 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 2009-02-13-02 (or later) to put this new protection into place. Protection for these vulnerabilities is automatically applied to the IPS rules 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-106228	CVE-2008-5416	Microsoft SQL Server sp_replwritevarbin Vulnerability	Recommended	Recommended
tln-106227	CVE-2009-0075	Microsoft Internet Explorer v7 Uninitialized Memory Corruption	Strict	--
tln-106218	CVE-2008-4255	Microsoft Visual Basic ActiveX Controls Animation Object	Strict	--
tln-106229	CVE-2009-0305	RIM Blackberry Application Web Loader ActiveX Buffer Overflow	Recommended	Recommended
tln-106230	CVE-2008-1770	Akamai Download Manager File Download to Arbitrary Location	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 106227
5. Enter **106227** in the search window
6. Double click on the rule **tln-106227 EXPLT: Microsoft Internet Explorer v7 Uninitialized Memory Corruption 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 Advisories	http://www.microsoft.com/technet/security/bulletin/MS09-004.msp http://www.microsoft.com/technet/security/bulletin/MS09-002.msp http://www.microsoft.com/technet/security/bulletin/MS08-070.msp http://www.microsoft.com/technet/security/advisory/960715.msp
Research in Motion Advisory	http://www.blackberry.com/btsc/KB16248
Akamai Advisory	http://www.akamai.com/html/support/security.html
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5416 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0075 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4255 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0305 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1770

Relevant TLN Rules: tln-106218, tln-106227 through tln-106230