

TopResponse Threat Advisory

Release Date: November 12, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Excel Field Sanitization Vulnerability (MS09-067,CVE-2009-3134).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Office Excel 2002 SP3; Microsoft Office Excel 2003 SP3; Microsoft Office Excel 2007 SP1 and SP2; Microsoft Office 2004 for Mac; Microsoft Office 2008 for Mac; Open XML File Format Converter for Mac; Microsoft Office Excel Viewer 2003 SP1, SP2, and SP3; Microsoft Office Compatibility Pack for Word, Excel, and Powerpoint 2007 File Formats SP1 and SP2.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

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

Advisory Impact: Prevention

Summary: Microsoft Excel supports the ability to store information in a spreadsheet file format. There is an exploitable defect in the way that Microsoft Office Excel parses the Excel field records contained within stored XLS files. The reported 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 XLS file.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-11-11-02 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" IPS Rule Set. In order to take advantage of the protection, customers should make sure the IPS rule tln-106285 is enabled in the IPS Rule Set used to inspect traffic that transfers Excel files to your infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3134

Relevant TLN Rules: tln-106285

Relevant TopResponse Protection Pack(s): 2009-11-11-02