

TopResponse Threat Advisory

Release Date: June 28, 2011.

Purpose: The Corero TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Excel WriteAV Remote Code Execution Vulnerability (MS11-045,CVE-2011-1278).

Corero Products: Top Layer IPS 5500 E-Series and later.

Vulnerable Infrastructure: Microsoft Office XP SP3,Microsoft Excel 2002 SP3,Microsoft Office 2003 SP3,Microsoft Excel 2003 SP3,Microsoft Office 2007 SP2,Microsoft Excel 2007 SP2,Microsoft Office 2010 (32-bit editions),Microsoft Excel 2010 (32-bit editions),Microsoft Office 2010 (64-bit editions),Microsoft Office 2004 for Mac,Microsoft Office 2008 for Mac,Microsoft Office for Mac 2011, and Open XML File Format Converter for Mac.

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 contains a vulnerability in the way records are parsed. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems 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 2011-06-27-02 (or later) to put this new protection into place. This will put into place protection for the Microsoft Excel WriteAV Remote Code Execution Vulnerability that will be applied to the "Strict Client Protection" IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-106366 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Excel infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Corero Support	http://www.corero.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS11-045.msp

Relevant IPS 5500 Rules: tln-106366.

Relevant TopResponse Protection Pack(s): 2011-06-27-02.