

TopResponse Threat Advisory

Release Date: September 6, 2011.

Purpose: The Corero TopResponse team is issuing an advisory, which provides information needed to provide protection against known attacks targeting the Microsoft Excel RTD Data Record Remote Code Execution Vulnerability (MS11-021,CVE-2011-0105).

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

Vulnerable Infrastructure: Microsoft Office XP SP3, Microsoft Office 2003 SP3, Microsoft Office 2007 SP2, Microsoft Office 2010 (32-bit editions), and Microsoft Office 2010 (64-bit editions).

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 implements parsing of various types of data records used in XLS files. There exists a vulnerability caused by an improperly initialized variable that is used as the length of a memcpy operation while parsing RTD data records in XLS files. 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: Corero recommends the following actions:

Download and apply Protection Pack 2011-09-02-01 (or later) to put this new protection into place. This will put into place protection against known attacks targeting the Microsoft Excel RTD Data Record Remote Code Corruption Vulnerability that will be applied to the "Recommended Client Protection" IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-022131 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/ms11-021.msp

Relevant IPS 5500 Rules: tln-022131.

Relevant TopResponse Protection Pack(s): 2011-09-02-01.