

TopResponse Threat Advisory

Release Date: August 11, 2011.

Purpose: The Corero TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Report Viewer XSS Vulnerability (MS11-067,CVE-2011-1976).

Corero Products: Top Layer IPS 5500 and later.

Vulnerable Infrastructure: Microsoft Visual Studio 2005 SP1 and Microsoft Report Viewer 2005 SP1 Redistributable Package.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow information disclosure

Advisory Impact: Prevention

Summary: Microsoft Report Viewer package implements controls for viewing reports created using Microsoft reporting technology. There exists a vulnerability in the way Microsoft Report Viewer validates parameters in a data source. The reported vulnerability could allow a remote attacker to inject a script into a user's browser by enticing the user to click on a specially crafted web link. The IPS 5500 provides proactive protection against known attacks targeting this vulnerability.

Recommended Action: Corero recommends the following actions:

Ensure that the rule tln-102078, "EXPLT: HTTP URI Query Value Matches Specified Filter", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft Report Viewer infrastructure. The rule is currently enabled in the "Strict Client Protection" and "Recommended Server Protection" IPS Rule Sets.

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/MS11-067.msp

Relevant IPS 5500 Rules: tln-102078.