

## TopResponse Threat Advisory

**Release Date:** November 8, 2011.

**Purpose:** The Corero TopResponse team is informing customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Windows TCP/IP Stack Reference Counter Overflow Vulnerability (MS11-083,CVE-2011-2013).

**Corero Products:** Top Layer IPS 5500 and later.

**Vulnerable Infrastructure:** Microsoft Windows Vista SP2, Microsoft Windows Vista x64 Edition SP2, Microsoft Windows Server 2008 for 32-bit Systems SP2, Microsoft Windows Server 2008 for x64-based Systems SP2, Microsoft Windows Server 2008 for Itanium-based Systems SP2, Microsoft Windows 7 for 32-bit Systems and Microsoft Windows 7 for 32-bit Systems SP1, Microsoft Windows 7 for x64-based Systems and Microsoft Windows 7 for x64-based Systems SP1, Microsoft Windows Server 2008 R2 for x64-based Systems and Microsoft Windows Server 2008 R2 for x64-based Systems SP1, Microsoft Windows Server 2008 R2 for Itanium-based Systems and Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1.

**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 Windows TCP/IP Stack implementation contains a vulnerability in the way continuous flow of specially crafted UDP packets is processed. The reported vulnerability could allow a remote attacker to execute arbitrary code in kernel mode on the vulnerable infrastructure components by sending specially crafted UDP packets to vulnerable Microsoft Windows systems. The IPS 5500 provides proactive protection against known attacks targeting this vulnerability.

**Recommended Action:** Corero recommends the following actions:

Create a firewall policy on the IPS, using blocking rules and application rate limiting functionality to rate limit or block, where appropriate, UDP traffic to unused UDP ports on your Windows systems.

**References:** Use the following sources for additional information:

Additional Information	Location
Corero Support	<a href="http://www.corero.com/support">http://www.corero.com/support</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/Bulletin/MS11-083.msp">http://www.microsoft.com/technet/security/Bulletin/MS11-083.msp</a>

**Relevant IPS 5500 Rules:** tln-002005.