

TopResponse Threat Advisory

Release Date: August 24, 2011.

Purpose: The Corero TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft ICMP Denial-of-Service Vulnerability (MS11-064,CVE-2011-1871).

Corero Products: Top Layer IPS 4.X 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 Windows 7 for 32-bit Systems SP1,Microsoft Windows 7 for x64-based Systems and Windows 7 for x64-based Systems SP1,Microsoft Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems SP1,Microsoft Windows Server 2008 R2 for Itanium-based Systems and 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 perform a Denial-of-Service attack against vulnerable systems

Advisory Impact: Prevention

Summary: The Microsoft Windows TCP/IP stack implementation contains a vulnerability in the way sequences of ICMP messages are processed. The reported vulnerability could allow an attacker to perform a Denial-of-Service attack against vulnerable Microsoft Windows systems causing the systems to stop responding and reboot by sending a set of specially crafted ICMP messages.

Recommended Action:

Per Microsoft guidance, to mitigate the impact of the vulnerability, the recommendation is to block all ICMP traffic to the vulnerable infrastructure by adding a row to your Firewall and IPS Policies. Note that, since ICMP messages can be used by TCP to reduce fragmentation, this change may have an impact on TCP throughput.

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/ms11-064.msp