Threat Update Service* Advisory

May 14, 2013

Purpose: The Corero Security Active Response Team informs customers that the IPS 5500 has proactive coverage against potential attacks targeting the Microsoft HTTP.SYS Denial-of-Service Vulnerability.

Issue: The HTTP protocol stack in Windows does not properly parse the HTTP header thereby allowing a remote attacker to cause a denial of service via a specially crafted header.

Recommended Action: Enable the specified rule and ensure that the rule is used to inspect traffic to the affected product infrastructure.

Issue Identifier	CVE-2013-1305, MS13-039
Advisory	https://technet.microsoft.com/en-us/security/bulletin/ms13-039
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to cause a denial of service of the affected system.
Affected Products	Windows 8 Windows 2012 Windows RT
Corero Products	IPS 5500 and later.
Associated Rule	tln-102062
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” and “Recommended Server Protection” rule sets.

* previously called TopResponse

https://support.corero.com Corero Network Security, Inc.
One Cabot Road, Hudson, MA 01749 +1 978.212.1500 • Fax +1 978.212.1600
• USA • Japan • Asia Pacific • EMEA