Threat Update Service* Advisory

June 10, 2014

Purpose: The Corero Security Active Response Team informs customers that the IPS 5500 has proactive coverage against attacks targeting the Lync Server Content Sanitization Vulnerability.

Issue: Microsoft Lync Server does not properly handle malicious JavaScript elements within a specially crafted URL which can lead to a cross-site scripting attack. This could allow an attacker to potentially execute scripts in the context of the victim and gain access to sensitive information from web sessions.

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

Issue Identifier	CVE-2014-1823, MS14-032
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms14-032
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain access to sensitive information from an unprotected system.
Affected Products	Microsoft Lync Server 2010 Microsoft Lync Server 2013
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.82 (build 002 and later), v6.80 (build 035 and later).
Associated Rule	tln-102078
Associated Rule Set	This rule is enabled in the “Recommended Server Protection” and “Strict Client Protection” rule sets.

* previously called TopResponse

http://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