Threat Update Service* Advisory

Protection Pack 2014-05-30-01 Released May 30, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Symantec Workspace Streaming Arbitrary File Upload Vulnerability.

Issue: A file upload vulnerability exists in Symantec Workspace Streaming. This could allow an attacker to upload arbitrary files to the victim's machine via a specially crafted XMLRPC request over HTTP. An attacker who successfully exploited this vulnerability could gain unauthorized privileged access to the affected system.

Recommended Action: Apply the specified Protection Pack (or any later one) and ensure the associated rule is used to inspect traffic to the affected product infrastructure.

Issue Identifier	CVE-2014-1649
Advisory	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20140512_00
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to upload arbitrary files to an unprotected system.
Affected Products	Symantec Workspace Streaming (SWS) before 7.5.0.749
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-025261
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

 Copyright 2014. All Rights Reserved.