Threat Update Service* Advisory

Protection Pack 2014-05-08-01 Released May 9, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the SEPMSPC Secars.dll CVE-2013-1612 Buffer Overflow Vulnerability.

Issue: A buffer overflow vulnerability exists in secars.dll as used in the Symantec Endpoint Protection Manager and the Symantec Endpoint Protection Center. This could allow an attacker to execute arbitrary code on the victim's machine via a specially crafted HTTP request. An attacker who successfully exploited this vulnerability could take complete control of an 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-2013-1612
Advisory	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20130618_00
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Symantec Endpoint Protection Manager (SEPM) 12.1.x before 12.1.3 Symantec Endpoint Protection Center (SPC) Small Business Edition 12.0.x
Corero Products	IPS 5500 E-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-106858
Associated Rule Set	This rule is automatically enabled in the "Strict Server Protection" rule set.

* previously called TopResponse

