Threat Update Service* Advisory

Protection Pack 2014-01-17-02 Released January 17, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the HP SiteScope issueSiebelCmd Remote Code Execution Vulnerability.

Issue: A remote code execution vulnerability exists in the APISiteScopeImpl SOAP service in HP SiteScope. This could allow an attacker to execute arbitrary code on the victim's machine via a direct request to the issueSiebelCmd method.

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-2013-4835
Advisory	https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c03969435
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	HP SiteScope 10.1x HP SiteScope 11.x before 11.22
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-025227
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

