Threat Update Service* Advisory

Protection Pack 2012-12-28-04 Released December 28, 2012

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

Issue: The UploadManagerServlet in HP SiteScope does not properly validate JSP's. This could allow an attacker to execute arbitrary code on the victim's machine by embeddding a malicious payload within a JSP. 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-2012-3264
Advisory	http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	HP SiteScope 11.10 through 11.12
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-022163
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* 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