Threat Update Service* Advisory

April 26, 2013

Purpose: The Corero Security Active Response Team informs customers that the IPS 5500 has proactive coverage against known attacks targeting the HP System Management Homepage 'iprange' Parameter Remote Code Execution Vulnerability.

Issue: A remote code execution vulnerability exists in the HP System Management Homepage thereby allowing an attacker to execute arbitrary code on the remote system as it does not properly validate the iprange parameter on a request against /proxy/DataValidation. This could allow an attacker to possibly take complete control of an affected system.

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

Issue Identifier	BID: 58817
Advisory	http://www.securityfocus.com/bid/58817/discuss
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the affected system.
Affected Products	HP System Management Homepage 7.1.1 and earlier
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-028001
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” and “Recommended Server Protection” rule sets.

* 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