

Threat Update Service* Advisory

May 30, 2014

Purpose: The Corero Security Active Response Team informs customers that the IPS 5500 has proactive coverage against attacks targeting the HP Release Control Authenticated XXE Vulnerability.

Issue: An XML External Entity (XXE) processing vulnerability exists in the dashboard XML import mechanism of HP Release Control. This could allow an attacker to read arbitrary files from the file system and gain access to sensitive information.

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

Issue Identifier	CNS-0100
Link	http://seclists.org/fulldisclosure/2014/May/77
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to read arbitrary files from an unprotected system.
Affected Products	HP Release Control 9.20.0000, Build 395
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-025250
Associated Rule Set	This rule is enabled in the "Strict Server Protection" rule set.

* previously called TopResponse

<http://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 Copyright 2014. All Rights Reserved.