Threat Update Service* Advisory

Protection Pack 2013-12-03-01 Released December 4, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the HP Intelligent Management SOM Account Add/Delete/Modify Vulnerability.

Issue: An authentication bypass vulnerability exists in the HP IMC Branch Intelligent Management System Software Module. This could allow an attacker to create, delete or modify accounts remotely via a specially crafted request.

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-2013-4824
Advisory	https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c03943547
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to bypass authentication on an unprotected system.
Affected Products	HP Intelligent Management Center (iMC) HP IMC Branch Intelligent Management System Software Module
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-025212
Associated Rule Set	This rule needs to be specifically enabled.

* 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