

## **Threat Update Service\* Advisory**

### **Protection Pack 2012-10-26-04 Released October 26, 2012**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the HP OpenView Performance Agent Coda Buffer Overflow Vulnerability.

**Issue:** A buffer overflow vulnerability exists in the HP Operations Agent. This could allow an attacker to execute arbitrary code on the victim's machine. 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.

<b>Issue Identifier</b>	CVE-2012-2019, CVE-2012-2020
<b>Vendor Advisory</b>	<a href="http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769">http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769</a>
<b>Risk Assessment</b>	Critical Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
<b>Affected Products</b>	HP Operations Agent before 11.03.12
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tln-022158
<b>Associated Rule Set</b>	This rule is automatically enabled in the "Strict 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 Copyright 2012. All Rights Reserved.