

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

### **Protection Pack 2012-11-20-02 Released November 20, 2012**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting HP Data Protector Express Create New Folder Buffer Overflow Vulnerability.

**Issue:** A remote code execution vulnerability exists in HP Data Protector Express. 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-2012-0124
<b>Advisory</b>	<a href="http://www.securityfocus.com/bid/52431">http://www.securityfocus.com/bid/52431</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 Data Protector Express 5.0.00 before build 59287 HP Data Protector Express 6.0.00 before build 11974
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tln-106543
<b>Associated Rule Set</b>	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 Copyright 2012. All Rights Reserved.