

## Threat Update Service\* Advisory Protection Pack 2014-09-26-01 Released September 26, 2014

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the GNU Bash CVE-2014-7169 Remote Code Execution Vulnerability.

**Issue:** Bash processes trailing strings after function definitions in the values of environment variables. This could allow an attacker to execute arbitrary commands on the victim's machine 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.

<b>Issue Identifier</b>	CVE-2014-7169
<b>Advisory</b>	<a href="http://www.securityfocus.com/bid/70137">http://www.securityfocus.com/bid/70137</a>
<b>Risk Assessment</b>	Critical Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
<b>Affected Products</b>	GNU Bash through 4.3
<b>Corero Products</b>	IPS / DDS 5500 EC-Series and IPS / DDS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (DDS build 044 and earlier, IPS build 035 and later), v6.82 (build 003 and later).
<b>Associated Rule</b>	tln-106933, tln-105001
<b>Associated Rule Set</b>	These rules need to be enabled and might require configuration.

\* 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.