

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

### **Protection Pack 2012-12-06-04 Released December 6, 2012**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle MySQL GRANT FILE Stack Based Buffer Overrun Vulnerability.

**Issue:** A stack buffer overflow vulnerability exists in Oracle MySQL. This could allow a remote authenticated attacker to execute arbitrary code on the victim's machine via a long argument to the GRANT FILE command. 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-2012-5611
<b>Advisory</b>	<a href="http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5611">http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5611</a>
<b>Risk Assessment</b>	Important Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to gain control of an unprotected system.
<b>Affected Products</b>	MySQL 5.5.19 and 5.1.53 MariaDB 5.5.2.x before 5.5.28a MariaDB 5.3.x before 5.3.11 MariaDB 5.2.x before 5.2.13 MariaDB 5.1.x before 5.1.66
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tln-106550
<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.