# Threat Update Service* Advisory

## Protection Pack 2012-12-21-02 Released December 21, 2012

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle MySQL Server Privilege Escalation Vulnerability.

**Issue:** A configuration issue in Oracle MySQL on Microsoft Windows can cause unprivileged users to create files as the adminsitrator. This could allow a remote authenticated 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.

| | |
|---|---|
| **Issue Identifier** | CVE-2012-5613 |
| **Advisory** | http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5613 |
| **Risk Assessment** | Important Vulnerability |
| **Threat Impact** | Remotely exploitable vulnerability that could allow an attacker to gain control of an unprotected system. |
| **Affected Products** | MySQL 5.5.19<br>MariaDB 5.5.28a |
| **Corero Products** | IPS 5500 E-Series and later. |
| **Associated Rule** | tln-106549 |
| **Associated Rule Set** | This rule is automatically enabled in the "Recommended Server Protection" rule set. |

* previously called TopResponse

 