Threat Update Service* Advisory

Protection Pack 2014-03-21-01 Released March 21, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the OracleDB TNS Listener CVE-2012-1675 Remote Poisoning Vulnerability.

Issue: A remote poisoning vulnerability exists in the Oracle Database Server. This could allow an attacker to execute arbitrary commands on the machine and conduct a man-in-the-middle attack to hijack database connections.

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-2012-1675
Advisory	https://blogs.oracle.com/security/entry/security_alert_for_cve_2012
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to hijack database connections.
Affected Products	Oracle Database 11g 11.1.0.7, 11.2.0.2, and 11.2.0.3, and 10g 10.2.0.3, 10.2.0.4, and 10.2.0.5
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-106830
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” rule set.

* previously called TopResponse

