Threat Update Service* Advisory

Protection Pack 2013-04-26-02 Released April 26, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the PostgreSQL Database Name Command Line Flag Injection Vulnerability.

Issue: An argument injection vulnerability exists in PostgreSQL. This could allow an attacker to execute arbitrary code on the victim's machine via a connection request using a database name that begins with a hyphen . 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-2013-1899
Advisory	http://www.postgresql.org/support/security/faq/2013-04-04/
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	PostgreSQL 9.2.x before 9.2.4 PostgreSQL 9.1.x before 9.1.9 PostgreSQL 9.0.x before 9.0.13
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025167
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

