Threat Update Service* Advisory

Protection Pack 2013-03-29-03 Released March 29, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Firebird Relational Database CNCT Group Number Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in Firebird as it does not properly validate the group number in CNCT information. This could allow a remote attacker to execute arbitrary code on the system and possibly take complete control of the affected system via a crafted packet to TCP port 3050.

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-2013-2492
Advisory	http://tracker.firebirdsql.org/browse/CORE-4058
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system.
Affected Products	Firebird 2.1.3 through 2.1.5 before 18514 Firebird 2.5.1 through 2.5.3 before 26623
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025163
Associated Rule Set	This rule is automatically enabled in the “Recommended 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