Threat Update Service* Advisory

Protection Pack 2014-04-04-01 Released April 4, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the IBM Tealeaf CX CVE-2013-6719 OS Command Injection Vulnerability.

Issue: A remote command execution vulnerability exists in IBM Tealeaf CX. This could allow an attacker to execute arbitrary commands on the victim's machine via shell metacharacters in the testconn_host parameter.

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-2013-6719
Advisory	https://tealeaf.support.ibmcloud.com/FileManagement/Download/19eb90ffb8334b398684b4350edc4b7a
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary commands on an unprotected system.
Affected Products	IBM Tealeaf CX 7.x, 8.x through 8.6, 8.7 before FP2, and 8.8 before FP2
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-106838
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