

## **Threat Update Service\* Advisory**

### **Protection Pack 2012-09-28-03 Released September 28, 2012**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the IBM Lotus Quickr qp2.cab ActiveX Control Stack Buffer Overflow Vulnerability.

**Issue:** A stack buffer overflow vulnerability exists in qp2.cab in IBM Lotus Quickr. This could allow an attacker to execute arbitrary code on the remote machine by sending a very long argument to the Import\_Times method. 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.

<b>Issue Identifier</b>	CVE-2012-2176
<b>Vendor Advisory</b>	<a href="http://www.ibm.com/support/docview.wss?uid=swg21596191">http://www.ibm.com/support/docview.wss?uid=swg21596191</a>
<b>Risk Assessment</b>	Critical Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
<b>Affected Products</b>	IBM Lotus Quickr 8.2 before 8.2.0.27-002a for Domino
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tln-022154
<b>Associated Rule Set</b>	This rule is automatically enabled in the "Recommended Client 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 Copyright 2012. All Rights Reserved.