Threat Update Service* Advisory

Protection Pack 2013-01-03-01 Released January 7, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the IBM Lotus Notes URL Handler Remote Code Execution Vulnerability.

Issue: The URL handler in IBM Lotus Notes does not properly validate the notes:// URL. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted link. 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-2012-2174
Vendor Advisory	http://www.ibm.com/support/docview.wss?uid=swg21598348
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	IBM Lotus Notes 8.x before 8.5.3 FP2
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025155
Associated Rule Set	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