Threat Update Service* Advisory

Protection Pack 2012-09-25-02 Released September 25, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the IBM Lotus iNotes Upload Module ActiveX Control Buffer Overflow Vulnerability.

Issue: A buffer overflow vulnerability exists in dwa85W.dll in IBM Lotus iNotes. This could allow an attacker to execute arbitrary code on the remote machine by sending a very long argument to the Attachment_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.

Issue Identifier	CVE-2012-2175
Vendor Advisory	http://www.ibm.com/support/docview.wss?uid=swg21596862
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 iNotes 8.5.x before 8.5.3 FP2
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-022153
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