Threat Update Service* Advisory

Protection Pack 2013-03-08-03 Released March 8, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the BigAnt Server DUPF Command Arbitrary File Upload Vulnerability.

Issue: A remote attacker can upload arbitrary files to the BigAntSoft BigAnt IM Message Server as it does not enforce any authentication. This could aid an attacker in carrying out further attacks.

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-2012-6274
Advisory	http://www.kb.cert.org/vuls/id/990652
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to upload arbitrary files and carry out further attacks.
Affected Products	BigAntSoft BigAnt IM Message Server
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025160
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” and “Recommended Client Protection” rule sets.

* previously called TopResponse

