Threat Update Service* Advisory
March 8, 2013

Purpose: The Corero Security Active Response Team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the BigAnt Server DUPF Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerabiity exists in AntDS.exe in BigAntSoft BigAnt IM Message Server. This could allow an attacker to execute arbitrary code on the victim's machine and possibly take complete control of the system via the userid component in a DUPF request.

Recommended Action: Enable the specified rule and ensure that the rule is used to inspect traffic to the affected product infrastructure.

Issue Identifier	CVE-2012-6275
Advisory	http://www.kb.cert.org/vuls/id/990652
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	BigAntSoft BigAnt IM Message Server
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-021027
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" and "Recommended Client Protection" rule sets.

* 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