Threat Update Service* Advisory
July 27, 2012

Purpose: The Corero Security Active Response Team informs customers that existing IPS 5500 security features provide proactive protection against potential attacks targeting the Asterisk HTTP Digest Denial-of-Service Vulnerability.

Issue: The Asterisk Manager Interface does not properly validate certain HTTP Digest Authentication headers which could lead to a stack buffer overflow. This could allow an attacker to cause a denial of service or potentially execute arbitrary code on the victim's machine.

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-2012-1184
Vendor Advisory	http://downloads.asterisk.org/pub/security/AST-2012-003.pdf
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to cause a denial of service or potentially execute arbitrary code on an unprotected system.
Affected Products	Asterisk Open Source 1.8.x prior to 1.8.10.1 Asterisk Open Source 10.x prior to 10.2.1
Corero Products	IPS 5500 4.X and later.
Associated Rule	tln-102049
Associated Rule Set	This rule is automatically enabled in the "Strict Server 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