Threat Update Service* Advisory
August 3, 2012

Purpose: The Corero Security Active Response Team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Samba Null Pointer Dereference Denial-of-Service Vulnerability.

Issue: A NULL pointer dereference vulnerability exists in smbd in Samba. This could allow an attacker to cause a denial of service on the victim's machine by sending specially crafted Negotiate Protocol and Session Setup AndX requests.

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-2010-1635
Vendor Advisory	http://git.samba.org/?p=samba.git;a=commit;h=25452a2268ac7013da28125f3df22085139af12d
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to cause a denial of service on an unprotected system.
Affected Products	Samba before 3.4.8 Samba 3.5.x before 3.5.2
Corero Products	IPS 5500 4.X and later.
Associated Rule	tln-005022
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