Threat Update Service* Advisory
October 26, 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 Perl-Based DCE/RPC IDL Compiler Remote Code Execution Vulnerability.

Issue: The RPC code generator in Samba does not properly validate the length of an array. This could allow an attacker to execute arbitrary code on the victim's machine by sending a specially crafted RPC request.

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-2012-1182
Vendor Advisory	https://www.samba.org/samba/security/CVE-2012-1182
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Samba 3.x before 3.4.16 Samba 3.5.x before 3.5.14 Samba 3.6.x before 3.6.4
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