Threat Update Service* Advisory

March 29, 2013

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

Issue: Windows NFS server does not properly handle a file operation on a read-only share. This could allow an attacker to cause a denial of service and cause the affected system to stop responding and restart.

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

Issue Identifier	CVE-2013-1281, MS13-014
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms13-014
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to cause a denial of service.
Affected Products	Windows Server 2008 R2 Windows Server 2012
Corero Products	IPS 5500 and later.
Associated Rule	tln-106051
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” and “Recommended Client Protection” rule sets.

* previously called TopResponse

