Threat Update Service* Advisory

Protection Pack 2014-01-31-01 Released January 31, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Nisuta Router Remote Management Web Interface Authentication Bypass Vulnerability.

Issue: An authentication bypass vulnerability exists in the remote management web interface of the Nisuta router. This could allow an attacker to gain complete control of the affected system via a "Cookie: :language=en" HTTP header.

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-2013-7282
Advisory	http://www.ampliasecurity.com/advisories/AMPLIA-ARA050913.txt
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain complete contrlol of an unprotected system.
Affected Products	Nisuta NS-WIR150NE router with firmware 5.07.41 and Nisuta NS-WIR300N router with firmware 5.07.36_NIS01
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-106780
Associated Rule Set	This rule is automatically enabled in the “Strict Server Protection” rule set.

* previously called TopResponse

