Threat Update Service* Advisory

Protection Pack 2013-03-22-02 Released March 26, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the 3S CODESYS SCADA Webserver Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in 3S CODESYS. This could allow a remote attacker to execute arbitrary code on the system and possibly take complete control of the affected system via a long URI to TCP port 8080.

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-2011-5007
Advisory	http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-336-01A.pdf
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system.
Affected Products	3S CoDeSys 3.4 SP4 Patch 2 and earlier
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-022140
Associated Rule Set	This rule is automatically enabled in the “Recommended 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