

Threat Update Service* Advisory
Protection Pack 2013-11-11-01 Released November 11, 2013

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

Issue: A stack buffer overflow exists in the CmpWebServer component in 3S CoDeSys. This could allow a remote attacker to execute arbitrary code on the vulnerable machine 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 an unprotected system.
Affected Products	3S CoDeSys 3.4 SP4 Patch 2 and earlier
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tIn-021504
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 Copyright 2013. All Rights Reserved.