Threat Update Service* Advisory

April 5, 2013

Purpose: The Corero Security Active Response Team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Siemens SIMATIC WinCC SCADA RegReader ActiveX Buffer Overflow Vulnerability.

Issue: The RegReader ActiveX control in Siemens WinCC does not properly validate parameters thereby allowing an attacker to execute arbitrary code on the remote system by exploiting a buffer overflow vulnerability. This could allow an attacker to possibly take complete control of an affected system by enticing the victim to open a specially crafted website.

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

Issue Identifier	CVE-2013-0676
Advisory	http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-714398.pdf
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the affected system.
Affected Products	Siemens WinCC before 7.2 SIMATIC PCS7 before 8.0 SP1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025140
Associated Rule Set	This rule is automatically enabled in the “Recommended Client 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