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 Sielco Sistemi Winlog SCADA Server Remote Overflow Vulnerability.

Issue: A stack buffer overflow exists in Sielco Sistemi Winlog Pro SCADA. This could allow a remote attacker to execute arbitrary code on the vulnerable machine via a specially crafted packet on TCP port 46824 that triggers an incorrect file-open attempt by the _TCPIPS_BinOpenFileFP function.

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-2012-4353
Advisory	http://www.sielcosistemi.com/en/news/index.html?id=69
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Sielco Sistemi Winlog Pro SCADA before 2.07.17 Winlog Lite SCADA before 2.07.17
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	tln-021503
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