Threat Update Service* Advisory

Protection Pack 2013-12-19-02 Released December 20, 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 vulnerability exists in Sielco Sistemi Winlog Pro. This could allow an attacker to execute arbitrary code on the victim's machine via a crafted 0x02 opcode packet to TCP port 46823. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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-2011-0517
Advisory	http://www.kb.cert.org/vuls/id/496040
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Sielco Sistemi Winlog Pro 2.07.00 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	tln-021511
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