Threat Update Service* Advisory

Protection Pack 2013-04-05-02 Released April 5, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Schneider Electric IGSS Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the Schneider Electric Interactive Graphical SCADA System (IGSS). This could allow a remote attacker to execute arbitrary code on the system and possibly take complete control of the affected system by sending crafted data on TCP port 12397.

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-2013-0657
Advisory	http://www.us-cert.gov/control_systems/pdf/ICSA-13-018-01.pdf
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system.
Affected Products	Schneider Electric Interactive Graphical SCADA System (IGSS) 10 and earlier
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-022166
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