Threat Update Service* Advisory

April 12, 2013

Purpose: The Corero Security Active Response Team informs customers that the IPS 5500 has proactive coverage against known attacks targeting the Scadatec Procyon Telnet Service Remote Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the Core Server HMI Service (Coreservice.exe) in Scadatec Limited Procyon thereby allowing an attacker to execute arbitrary code on the remote system. This could allow an attacker to possibly take complete control of an affected system by sending a very long password on TCP port 23.

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

Issue Identifier	CVE-2011-3322
Advisory	http://www.uscert.gov/control_systems/pdf/ICSA-11-216-01.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	Scadatec Limited Procyon SCADA 1.06
Corero Products	IPS 5500 and later.
Associated Rule	tln-009003 and tln-009009
Associated Rule Set	These rules are automatically enabled in the “Strict Client Protection” and “Strict Server Protection” rule sets.

* 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