Threat Update Service* Advisory

Protection Pack 2014-06-05-01 Released June 6, 2014

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

Issue: A stack buffer overflow vulnerability exists in the Schneider Electric OPC Factory Server. This could allow an attacker to gain elevated privileges on the victim's machine by enticing the victim to open a specially crafted configuration file.

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-2014-0774
Advisory	http://download.schneider-electric.com/files?p_Doc_Ref=SEVD%202014-031-01
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain elevated privileges on an unprotected system.
Affected Products	Schneider Electric OPC Factory Server (OFS) TLXCDSUOFS33 - 3.35, TLXCDSTOFS33 - 3.35, TLXCDLUOFS33 - 3.35, TLXCDLTOFS33 - 3.35, and TLXCDLFOFS33 - 3.35
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-022192
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

