# Threat Update Service* Advisory

## Protection Pack 2014-04-24-06 Released April 25, 2014

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

**Issue:** A stack buffer overflow vulnerability exists in ModbusDrv.exe in Schneider Electric Modbus Serial Driver. This could allow an attacker to execute arbitrary code on the victim's machine via a large buffer-size value in a Modbus Application Header.

**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-2013-0662 |
| **Advisory** | http://download.schneider-electric.com/files?p_Doc_Ref=SEVD%202013-070-01 |
| **Risk Assessment** | Critical Vulnerability |
| **Threat Impact** | Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system. |
| **Affected Products** | Schneider Electric Modbus Serial Driver 1.10 through 3.2 |
| **Corero Products** | IPS 5500 E-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-106853 |
| **Associated Rule Set** | This rule is automatically enabled in the "Recommended Server Protection" rule set. |

* previously called TopResponse

http://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 