# Threat Update Service* Advisory

## Protection Pack 2014-07-24-01 Released July 25, 2014

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Yokogawa CS3000 CVE-2014-3888 Stack Buffer Overflow Vulnerability.

**Issue:** A stack buffer overflow vulnerability exists in the Yokogawa CENTUM CS. This could allow an attacker to execute arbitrary code on the victim's machine via a specially crafted packet. 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-2014-3888 |
| **Advisory** | http://www.yokogawa.com/dcs/security/ysar/YSAR-14-0002E.pdf |
| **Risk Assessment** | Critical Vulnerability |
| **Threat Impact** | Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system. |
| **Affected Products** | Yokogawa CENTUM CS<br>Exaopc R3.72.00 and earlier<br>B/M9000CS R5.05.01 and earlier<br>B/M9000 VP R7.03.01 and earlier |
| **Corero Products** | IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later). |
| **Associated Rule** | tln-025269 |
| **Associated Rule Set** | This rule is automatically enabled in the "Strict Server Protection" rule set. |

* previously called TopResponse

 