# Threat Update Service* Advisory

## Protection Pack 2013-03-22-02 Released March 26, 2013

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Honeywell HSC Remote Deployer ActiveX Remote Code Execution Vulnerability.

**Issue:** A remote code execution vulnerability exists in the ActiveX control in HscRemoteDeploy.dll. This could allow a remote attacker to execute arbitrary code on the system and possibly take complete control of the affected system by enticing the victim to open a specially crafted webpage.

**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-2013-0108 |
| **Advisory** | http://ics-cert.us-cert.gov/pdf/ICSA-13-053-02.pdf |
| **Risk Assessment** | Critical Vulnerability |
| **Threat Impact** | Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system. |
| **Affected Products** | Honeywell Enterprise Buildings Integrator (EBI) R310, R400.2, R410.1, and R410.2<br>SymmetrE R310, R410.1, and R410.2<br>ComfortPoint Open Manager (aka CPO-M) Station R100<br>HMIWeb Browser client packages |
| **Corero Products** | IPS 5500 E-Series and later. |
| **Associated Rule** | tln-025162 |
| **Associated Rule Set** | This rule is automatically enabled in the “Strict Client 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 