



## SoundPoint® IP Family Technical Bulletin – TB 18759

**Security Advisory relating to vulnerability on the HTTP server interface to SoundPoint IP phones.**

---

This information applies to:

- SoundPoint IP300, 301, 430, 500, 501, 600, 601 and IP 4000 phones running all SIP software revisions.
- 

### **SYMPTOMS**

A customer has reported two security issues that were uncovered using the Nessus security scan utility. These have been published at <http://secunia.com/advisories/22266/>

### **Description**

A vulnerability has been reported in the Polycom SoundPoint IP 301 VoIP Desktop Phone, which can be exploited by malicious people to cause a DoS (Denial of Service).

Sending a long URL to the embedded HTTP server or using the Nessus `http_fingerprinting_hmap.nasl` script can cause the phone to reboot. Additionally, it has been reported that the TCP port 42 is open and accepting connections.

The vulnerabilities have been reported in firmware version 1.4.1.0040. Other versions may also be affected.

### **CAUSE**

**Issue 1:** The “reboot issue” is related to the web-server interface which is an optional method for configuration of the SoundPoint IP phones. This port could be used for a Denial Of Service attack on the phone.

**Issue 2:** TCP port 42 is used for manufacturing purposes and is permanently disabled on first phone configuration cycle using a centralized provisioning model (FTP, TFTP, HTTP, HTTPS). The tester that reported the issue has likely run the test on an unconfigured phone or used the web server interface to configure the phone.



## **WORKAROUND**

**Issue 1:** To avoid the susceptibility to an attack through the HTTP port, this port can be disabled by setting `httpd.enabled=0` in the **sip.cfg** file.

**Issue 2:** Use a centralized provisioning server for phone configuration. Once the first provisioning cycle is completed, TCP port 42 will be closed.

## **STATUS**

**Issue 1:** This issue will be addressed in a future SIP software release.

**Issue 2:** Polycom will investigate whether the manufacturing process can be altered to avoid leaving this port open when products are shipped.