

## Description

### Polycom HDX® Family Technical Bulletin – TB SEC1101

Security Advisory relating to vulnerability of Polycom HDX video endpoints to malicious attack using the Sockstress tool developed by Outpost24.

---

This information applies to:

- HDX 4000, 6000, 7000, 8000, and 9000 series video endpoints.
- 

## SYMPTOMS

The Finnish CERT organization<sup>1</sup> notified Polycom of a vulnerability<sup>2</sup> that affects the TCP/IP stack of most operating systems (“OS”), including the OS in the Polycom HDX family of products.<sup>3</sup> The CERT announcement also referenced a tool called “Sockstress” developed by researchers from Outpost24, credited with the vulnerability discovery.

Polycom received a copy of the Sockstress tool from the Finnish CERT organization to evaluate its effect on Polycom HDX systems.

## CAUSE

A server-side syn-cookie is a method to avoid falling to a syn flood by adding an encoded hash to each syn/ack sent. The server can then let go of the connection and doesn’t have to leave resources open waiting for the ack. The developers of sockstress have taken this idea and turned it around. Sockstress builds the same syn-cookie “table”—albeit on the client side—so that they don’t have to spend resources on the connection.

Additional points on the tool/attack:

- An attacker issuing less than 40 packets per second could cause an HDX to reboot
- All HDX systems running code below versions 2.7.0 should be considered vulnerable to this denial-of-service attack.
- To date, there is no known method to use this attack for privilege escalation or to take control of the HDX system.

---

<sup>1</sup> <http://www.cert.fi/en/>

<sup>2</sup> <https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>

<sup>3</sup> Multiple versions of Linux and Windows are affected by this vulnerability. See <http://kbase.redhat.com/faq/docs/DOC-18730> (detailing RedHat’s disclosure that their distribution is vulnerable and providing mitigation.)

## WORKAROUND

Best practices for system protection, including access control lists for critical systems is the best method for reducing the attack plane. From the cert.fi advisory:

Since an attacker must be able to establish TCP sockets to affect the target, the attacks can not be spoofed. White-listing access to TCP services on routers and critical systems is the currently most effective means for mitigation.<sup>4</sup>

Since the most significant impact to Polycom devices occurs on ports 23, 24, and 5060, Polycom recommends disabling telnet and SIP unless these protocols are required. If these protocols are required, then access control lists should be setup on the network to limit access to trusted IP ranges.

## STATUS

Polycom has addressed this issue in version 3.0 of the HDX software, which is available from the Polycom Support site<sup>5</sup>. Release notes for this release are available from HDX 3.0 download page<sup>6</sup> web site.

## ACKNOWLEDGMENT

Polycom would like to thank the team a CERT-FI for alerting us to this vulnerability and working with us to confirm the attack.

## REFERENCES

See: <http://www.cert.fi/en/>

See: <http://www.outpost24.com/>

---

<sup>4</sup> <https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>

<sup>5</sup> <http://support.polycom.com/>

<sup>6</sup> [http://downloads.polycom.com/video/hdx/ReleaseNotes/hdx\\_RelNotes30\\_036b.pdf](http://downloads.polycom.com/video/hdx/ReleaseNotes/hdx_RelNotes30_036b.pdf)