

Description

Polycom HDX® Family Technical Bulletin – TB SEC1102

Security Advisory relating to vulnerability of Polycom HDX video endpoints to denial-of-service conditions caused by the Codenomicon testing suite.

This information applies to:

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

SYMPTOMS

The Finnish CERT organization¹ notified Polycom of the results of a series of tests conducted against the HDX line of video conferencing end-points using the Codenomicon tool suite. The HDX was susceptible to Denial-of-Service (“DoS”) conditions when running the SNMPv2 and H.323 anomaly test packages.

Polycom purchased the SNMPv2 and H.323 test packages from Codenomicon, and was able to verify the DoS conditions.

CAUSE

The Codenomicon tools are protocol specific robustness tests which issue tens of thousands of anomalous packets to the protocol. The tool tests whether the device under test is able to continue responding, using valid (non-anomalous packets).

Additional points on the test results:

- The SNMPv2 tool consists of 57,860 tests. Of which, CERT-FI reported the HDX failed 445 cases, with two resulting in a denial-of-service (#9096 and #21030)
- The H.323 tool consists of 45,370 tests. Of which, CERT-FI reported one denial-of-service on the HDX (#22645)

WORKAROUND

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

Since the most significant failures were seen on the SNMPv2 protocol stack, disabling SNMPv2 or using access control lists to limit access to trusted IP ranges should be considered.

¹ <http://www.cert.fi/en/>

STATUS

Polycom has spent considerable time and resources to upgrade both the SNMPv2 and H.323 stacks within the HDX family of CODECs.

- The SNMPv2 issues were addressed in HDX software version 2.6
- The H.323 issue was addressed in HDX software version 3.0

Due to the use of the Codenomicon tools, the most recent software release, 3.0, provides much more robust protocol implementations. Version 3.0 of the HDX software is available from the Polycom Support site². Release notes for this release are available from HDX 3.0 download page³ 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. Polycom would also like to thank the support team at Codenomicon for working with Polycom security staff to make the HDX line of CODECs more robust.

REFERENCES

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

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

² <http://support.polycom.com/>

³ http://downloads.polycom.com/video/hdx/ReleaseNotes/hdx_RelNotes30_036b.pdf