Vendor of the products: D-Link

Affected Device: D-Link DI-7300G+

Version: DI-7300G+ V19.12.25A1

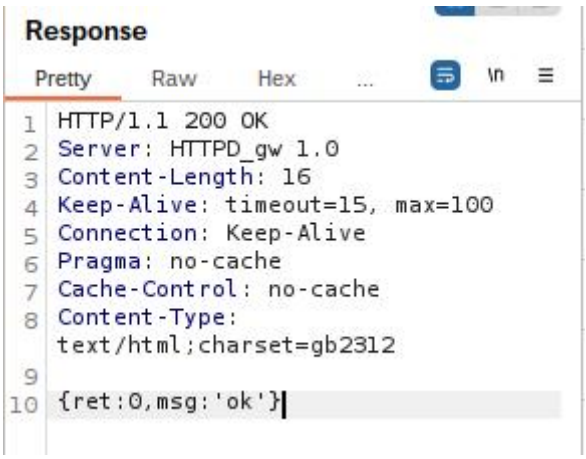
Firmware Download: http://www.dlink.com.cn/techsupport/ProductInfo.aspx?m=DI-7300G%2B

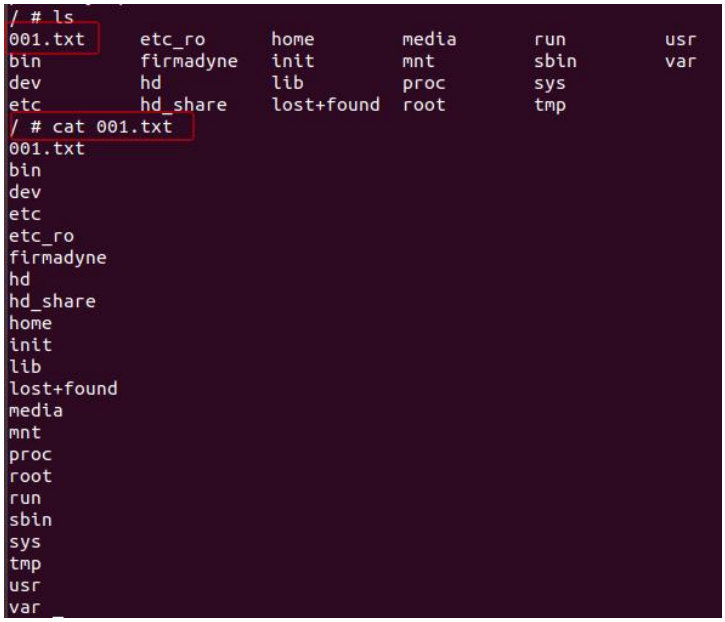
Vulnerability Description: A command injection vulnerability was discovered in D-Link DI-7300G+ V19.12.25A1, triggered by the url parameter in wget_test.asp. Attackers can exploit this vulnerability by constructing malicious packets to execute arbitrary commands, thereby gaining full control of the target device.

POC:

Vulnerability Effect:

It can be observed that the router receives the request and successfully executes the command.




/ # ls
001.txt etc_ro home media run usr
bin firmadyne init mnt sbin var
dev hd lib proc sys
etc hd_share lost+found root tmp
/ # cat 001.txt
001.txt
bin
dev
etc
etc_ro
firmadyne
hd
hd_share
home
init
lib
lost+found
media
mnt
proc
root
run
sbin
sys
tmp
usr
var

Vulnerability Cause:

The issue resides in the jhttpd component. In jhttpd, the program invokes the sub_45421C function to handle requests related to wget_test.asp. The program retrieves the values of the url and count parameters via httpd_get_parm. When the url parameter is non-empty and the count parameter value exceeds 0, it enters the vulnerability branch. Subsequently, the url parameter value is concatenated into the variable v8 using the sprintf function, and finally executed via the jhl_system function. Due to the lack of security checks on input data, attackers can execute arbitrary commands and fully control the device by constructing malicious parameters.