English

Threat Research Center　　　Threat Research　　　**Vulnerabilities**

VULNERABILITIES

6 New Vulnerabilities Found on D-Link Home Routers

6　min read

RELATED PRODUCTS

◆　**Next-Generation Firewall**

⚬　By:　　　　Gregory Basior

🗓　Published:　June 12, 2020

⊞　Categories:　　Threat Research , Vulnerabilities

🏷　Tags:　　　　D-Link , IoT , Wireless routers

Share　💬

Table of Contents

The vulnerabilities were found in the DIR-865L model of D-Link routers, which is meant for home network use. The current trend towards working from home increases the likelihood of malicious attacks against home networks, which makes it even more imperative to keeping our networking devices updated.

It is possible that some of these vulnerabilities are also present in newer models of the router because they share a similar codebase. The following are the six vulnerabilities found:

CVE-2020-13782: Improper Neutralization of Special Elements Used in a Command (Command Injection)

CVE-2020-13786: Cross-Site Request Forgery (CSRF)

CVE-2020-13785: Inadequate Encryption Strength

CVE-2020-13784: Predictable seed in pseudo-random number generator

CVE-2020-13783: Cleartext storage of sensitive information

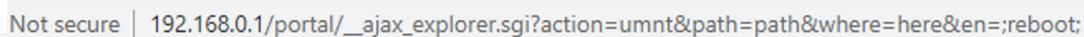CVE-2020-13787: Cleartext transmission of sensitive information

Different combinations of these vulnerabilities can lead to significant risks. For example, malicious users can sniff network traffic to steal session cookies. With this information, they can access the administrative portal for file sharing, giving them the ability to upload arbitrary malicious files, download sensitive files, or delete essential files. They can also use the cookie to run arbitrary commands to conduct a denial of service attack.

The Palo Alto Networks Next-Generation Firewalls with threat prevention are protected from this threat with custom signatures.

D-Link has released a patch that consumers are strongly recommended to install, which can be found at the following link: D-Link Announcement

CVE-2020-13782: Improper Neutralization of Special Elements Used in a Command (Command Injection)

The web interface for this router is controlled by the backend engine called cgibin.exe. Most requests for web pages are sent to this controller. If a request for scandir.sgi is made, a malicious actor can inject arbitrary code to be executed on the router with administrative privileges.


```
_  Not secure  │  192.168.0.1/portal/__ajax_explorer.sgi?action=umnt&path=path&where=here&en=;reboot;
```

Figure 1. Malicious http request

The above image shows a GET request that can be made to __ajax_explorer.sgi that will be sent to scandir.sgi and cause the router to reboot. This particular attack would lead to a denial of service.

For the attack to work, there must be four parameters in the request:

This attack requires authentication, but it can be conducted by stealing an active session cookie because the web page is vulnerable to cross site request forgery as well. As will be seen with later vulnerabilities, stealing a session cookie is trivial for an attacker.

CVE-2020-13786: Cross-Site Request Forgery (CSRF)

There are multiple pages on the router's web interface that are vulnerable to CSRF. This means that an attacker can sniff web traffic and use the session information to gain access to password-protected portions of the website without knowing the password.

The previous vulnerability already mentioned that the command injection can be conducted using CSRF. There is also a SharePort Web Access portal, which is an administrative web site for file sharing located on port 8181.

Below is a view of the traffic sniffed by a malicious user, in which they can use the `uid` to bypass logging in:

```
HTTP/1.1 200 OK
Server: Linux, WEBACCESS/1.0, DIR-865L Ver 1.09
Date: Fri, 28 Feb 2020 17:13:05 GMT
Connection: close
Content-Type: application/x-www-form-urlencoded
     ent-Length: 125

  status": "ok", "errno": null, "uid": "8ZFP4620og", "challenge": "84f9ecfa-786e-4406-baa6-156abd8650c5",
```

Figure 2. Cleartext transmission of UID

If the attacker were to navigate directly to the `folder_view.php` page, they can bypass the login screen but would have no functionality:
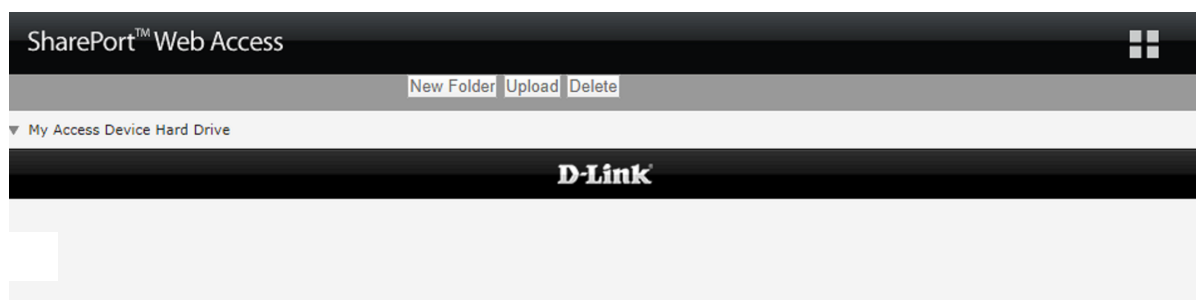

Figure 3. SharePort Web Access without authentication

If they were to simply change the value of the cookie to be the `uid` of the valid session, they would completely bypass authentication:
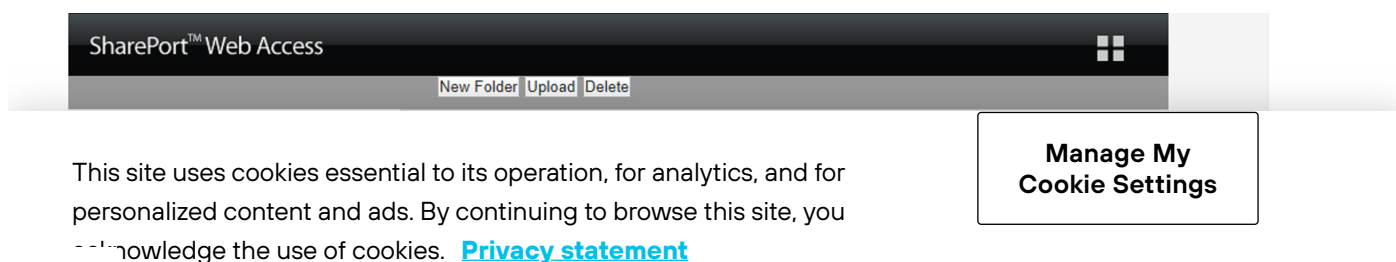

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. **Privacy statement**

Manage My Cookie Settings

Figure 4. SharePort Web Access with authentication

The attacker now has the ability to do three different things:

View the contents of all files.

Delete any or all files.

Upload new files, including malware.

CVE-2020-13785: Inadequate Encryption Strength

When a user logs into the SharePort Web Access portal on port 8181, there is enough information sent in clear text for a listening attacker to determine a user's password through a brute force attack.
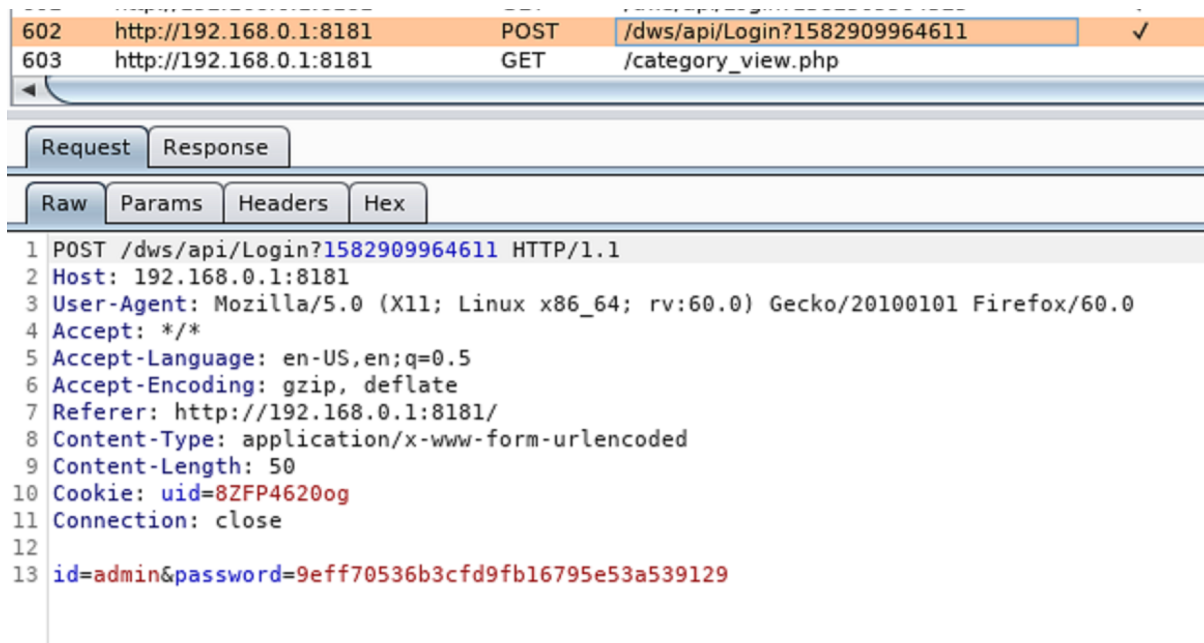
status": "ok", "errno": null, "uid": "8ZFP4620og", "challenge": "84f9ecfa-786e-4406-baa6-156abd8650c5",

Figure 5. Cleartext transmission of challenge

The above information is sent to the client from the router. The client will then calculate the password to send as follows:

MD5 HMAC of string equal to `username + challenge` with the actual password as the key.

The result of this calculation is sent back to the router in clear text:

```
602    http://192.168.0.1:8181         POST    /dws/api/Login?1582909964611                    ✓
603    http://192.168.0.1:8181         GET     /category_view.php
◄

  Request   Response

  Raw   Params   Headers   Hex

 1 POST /dws/api/Login?1582909964611 HTTP/1.1
 2 Host: 192.168.0.1:8181
 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
 4 Accept: */*
 5 Accept-Language: en-US,en;q=0.5
 6 Accept-Encoding: gzip, deflate
 7 Referer: http://192.168.0.1:8181/
 8 Content-Type: application/x-www-form-urlencoded
 9 Content-Length: 50
10 Cookie: uid=8ZFP4620og
11 Connection: close
12
13 id=admin&password=9eff70536b3cfd9fb16795e53a539129
```

completely offline.

CVE-2020-13784: Predictable Seed in Pseudo-Random Number Generator

There is an algorithm in the router's code-base that calculates the session cookie randomly, but the result is predictable. An attacker only needs to know the approximate time that a user logged on to determine the session cookie, even if it is protected with encryption.

Every time a user logs on, the router responds with a cookie, challenge, and public key:

Cleartext transmission of challenge, cookie and public key in D-Link Vulnerability

Figure 7. Cleartext transmission of challenge, cookie and public key

This information seems random, but it is created by a function called `get_random_string`. This function will seed the random number generated with the time of the login attempt. Thus, the result of the calculation can be predicted by an attacker who knows the time of the request.

Disassembly of random function seed in D-Link Vulnerability

Figure 8. Disassembly of random function seed

The result of this vulnerability is that even if the router is using HTTPS to encrypt session information, a sophisticated attacker can still determine the information necessary to conduct the CSRF attacks.

CVE-2020-13783: Cleartext Storage of Sensitive Information

The `tools_admin.php` page stores the admin password in clear text. In order for an attacker to get the

Figure 9. Tools_admin.php web page

Cleartext storage of password

Figure 10. Cleartext storage of password

CVE-2020-13787: Cleartext transmission of sensitive information

The `adv_gzone.php` page is used to set up a guest wifi network. There are multiple options available for the security on this network. One option is Wired Equivalent Privacy (WEP), which was deprecated in 2004, and not recommended to secure a wireless network. If the administrator chooses this option, the password will be sent over the network in clear text:

Figure 11. Cleartext transmission of password

In summary, the D-Link DIR-865L home wireless router has multiple vulnerabilities. Due to the number of people working from home, malicious actors have an incentive to attack routers meant for home networks.

These vulnerabilities can be used together to run arbitrary commands, exfiltrate data, upload malware, delete data or steal user credentials. These attacks are easiest to conduct if the router is set up to use HTTP, but a sophisticated attacker can still calculate the required session information if the router uses HTTPS.

Palo Alto Networks protects customers in the following ways:

Next-Generation Firewalls with threat prevention license can block the attacks with best practice via threat prevention signature `58410`.

Recommendations

Install the latest version of the firmware with patches. The firmware can be found on the D-Link website where they announced the vulnerabilities: D-Link Announcement.

Default all traffic to HTTPS to defend against session hijacking attacks.

Change the time zone on the router to defend against malicious actors who are calculating the randomly generated session id. You can find how to do that on D-Link's site.

Do not use this router to share sensitive information until it's patched.

Appendix

CVEs:

CVE-ID	Vulnerability type	Reference
CVE-2020-13782	Improper Neutralization of Special Elements Used in a Command (Command Injection)	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13782
CVE-2020-13783	Cleartext storage of sensitive information	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13783
CVE-2020-13784	Predictable seed in pseudo-random number generator	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13784

| CVE-2020 -1378 6 | Cross-Site Request Forgery | https://cve.mitre.org/cgi-bin/ cvename.cgi? name=CVE-2020-13786 |
| CVE-2020 -1378 7 | Cleartext transmission of sensitive information | https://cve.mitre.org/cgi-bin/ cvename.cgi? name=CVE-2020-13787 |

Back to top

TAGS

(**D-Link**)   (**IoT**)   (**Wireless routers**)

Threat Research Center   **Next: Threat Assessment: Hangover Threat Group**

Related Vulnerabilities Resources

ʍsletter

UNIT 42 Small Logo **Get updates from Unit 42**

Peace of mind comes from staving ahead of threats. Subscribe

Subscribe for email updates to all Unit 42 threat research.
By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.

Subscribe **Right Arrow**

Products and Services

Company

Popular Links

PAN logo

Privacy

Trust Center

Terms of Use

Documents

Copyright © 2025 Palo Alto Networks. All Rights Reserved

Youtube Podcast Facebook LinkedIn Twitter

EN