6 New Vulnerabilities Found on D-Link Home Routers

By Gregory Basior
June 12, 2020 at 6:00 AM
Category: Unit 42
Tags: D-Link, IoT, vulnerabilities, Wireless routers

Executive Summary

On February 28, 2020, Palo Alto Networks' Unit 42 researchers discovered six new vulnerabilities in D-Link wireless cloud routers running their latest firmware.

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.

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.

- **where**: this can be anything
- **en**: this parameter is where the command injection occurs. In this case `;reboot;` causes the router to restart.

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 a
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 administrat
8181.

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

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:

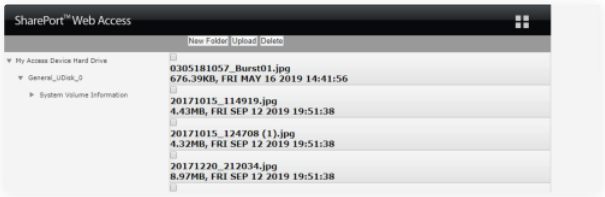


Figure 4. SharePort Web Access with authentication

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

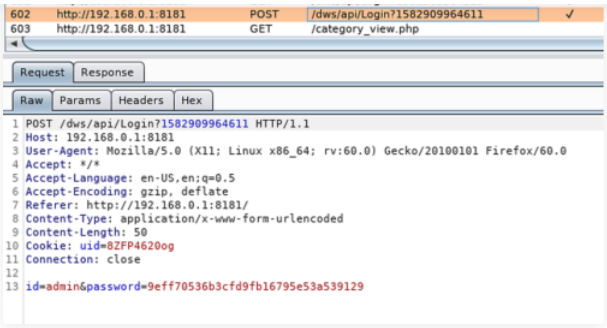
When a user logs into the SharePort Web Access portal on port 8181, there is enough information sent in clear text for a listening attacker to determine a user's password through a brute force attack.

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:



By sniffing this handshake, the attacker now has access to the following information:

- The data input for the MD5 HMAC algorithm = `id + challenge`
- The result of the hashing algorithm = `password`

With this information, the attacker can determine the actual password by conducting a brute force attack 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:

```
<LoginResponse xmlns="http://purenetworks.com/HNAP1/">
    <LoginResult>OK</LoginResult>
    <Challenge>CTgQhI1JzpeGgvGcaBa</Challenge>
    <Cookie>pNTX9D819</Cookie>
    <PublicKey>CPdevmp3nybxPFL5VLO</PublicKey>
</LoginResponse>
```

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.

```
00410068 40 82 99 8f    lw      t9,-0x7dc0(gp)=>->time
0041006c 00 00 00 00    nop
00410070 09 f8 20 03    jalr    t9=>time
00410074 00 00 00 00    _nop
00410078 10 00 dc 8f    lw      gp,local_18(s8)
0041007c 21 20 40 00    move    a0,v0
00410080 80 80 99 8f    lw      t9,-0x7f80(gp)=>->srand
00410084 00 00 00 00    nop
00410088 09 f8 20 03    jalr    t9=>srand
```

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 password, they would require physical access to a machine that is logged on. Physical access is necessary because the credentials are not sent in clear text over the wire. With physical access, they can see the password by viewing the HTML source of the page:

Figure 9. Tools_admin.php web page

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:

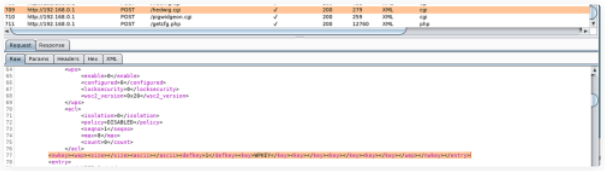


Figure 11. Cleartext transmission of password

Malicious users sniffing network traffic can see the password used for the guest network.

Conclusion

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

13786		
CVE-2020-13787	Cleartext transmission of sensitive information	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13787

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

Email address

Subscribe

I'm not a robot

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.