BLOGS & STORIES

SpiderLabs Blog

Attracting more than a half-million annual readers, this is the security community's go-to destination for technical breakdowns of the latest threats, critical vulnerability disclosures and cutting-edge research.

D-Link: Multiple Security Vulnerabilities Leading to RCE

December 17, 2020 Harold Zang

On the 30th of October, D-Link published a support announcement and released a new firmware to patch five vulnerabilities that Harold Zang, Technical Security Specialist at Trustwave, identified on the DSL-2888A router. These security vulnerabilities could allow a malicious Wi-Fi or local network user to gain unauthorised access to the router web interface, obtain the router password hash, gain plaintext credentials, and execute system commands on the router.

Finding-1: Insufficient Authentication (CVE-2020-24579)

The router web portal has insufficient authentication in place allowing access to any authenticated administrative page without the requirement to have the correct password. A malicious user located on the trusted network can directly browse to any authenticated administrative page with invalid credentials.

1. Browse to the router web interface: http://192.168.1.1/
2. Submit any strings as password
3. The application will inform the user that the password is invalid, however, a valid access session is achieved
4. Browse to any authenticated page. For example: /WiFi.shtml.

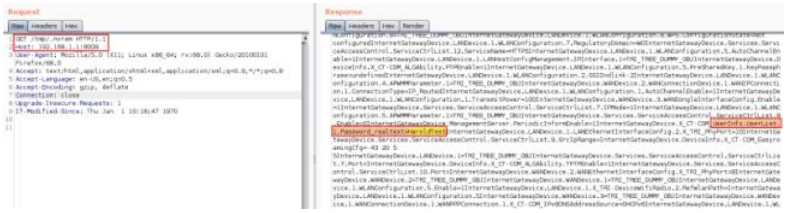
The following video demonstrates this vulnerability:

00:49

Finding-2: Information Leakage (CVE-2020-24577)

Upon establishing connection to the network either via physical connection or via wireless access, a malicious user can obtain the Internet provider connection username and password in plaintext, and the wireless router login username and password in plaintext by directly browsing to the following URLs:

http://DeviceIP:8008/tmp/cfg/lib_cfg_cfgcmd
http://DeviceIP:8008/tmp/.nvram



(https://npercoco.typepad.com/.a/6a0133f264aa62970b026bdea447e3200c-pi)

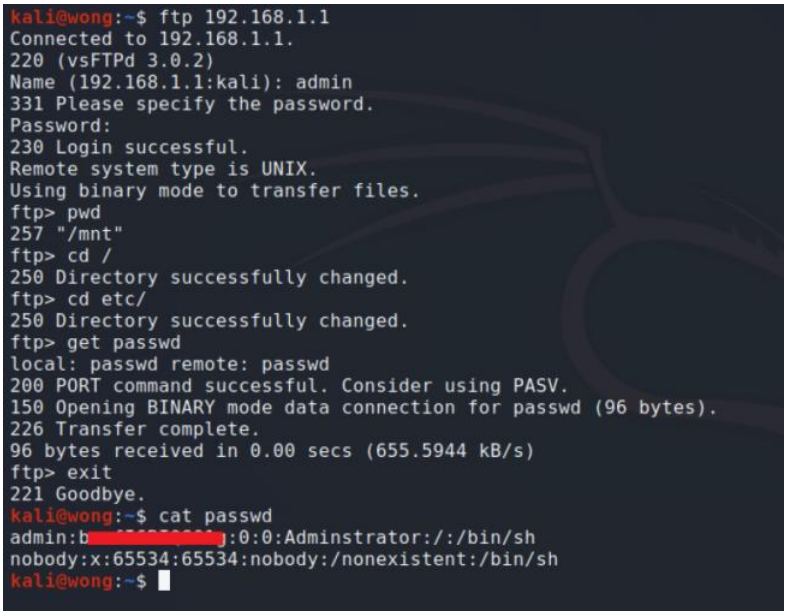
Finding-3: FTP Misconfiguration (CVE-2020-24578)

The D-Link DSL-2888A router has a file sharing functionality that allows users to share fileswith other network users via inserting an external drive onto the router. This is then shared via FTP (File Transfer Protocol). However, FTP service allows a network user to escape the shared folder to access the router file system and download other files located on the root folder.

The following provides an example for downloading the “passwd”:
Use the following command on an FTP client to connect to the FTP service with valid credentials (obtained from Finding-2).
ftp <DeviceIP>

Use the following command to navigate to the root folder.
ftp>cd /

Use the following command to download the password hash file.
ftp>cd etc/
ftp>get passwd



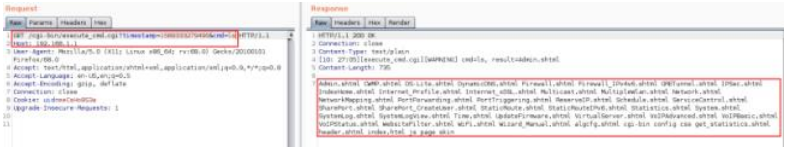
(https://npercoco.typepad.com/.a/6a0133f264aa62970b026be42336e1200d-pi)

The attacker must first obtain the FTP credentials. Finding-2 disclosed the credential in plaintext.

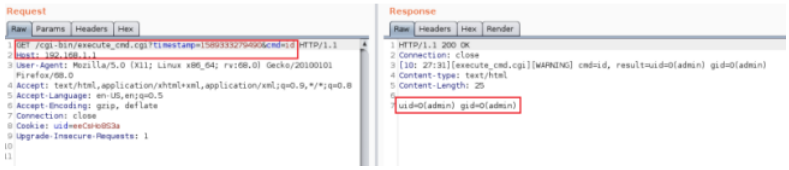
Finding-4: Hidden Functionality (CVE-2020-24581)

An authenticated user can to execute Linux operation system commands in the router via hidden functionality not available on the router’s web portal interface.

The following is a Proof of Concept URL:
http://DeviceIP/cgi-bin/execute_cmd.cgi?timestamp=1589333279490&cmd=ls



(https://npercoco.typepad.com/.a/6a0133f264aa62970b026be4233680200d-pi)



(https://npercoco.typepad.com/.a/6a0133f264aa62970b026bdea4482c200c-pi)

The ability to execute operation system commands on a router will allow an attacker to monitor network traffic to steal sensitive data including login credentials, this might also allow a malicious user to install backdoors on the router.

Although exploitation of this requires authentication, Finding-1 provides a way to bypass the authentication.

Finding-5: Improper Authentication (CVE-2020-24580)

The last vulnerability was another insufficient authentication vulnerability. The router uses the source IP address of a connecting user to perform authentication. The allows a malicious user to "spoof" the IP address of a legitimate user with a valid session by changing their IP address to that of an administrator user, to browse to any authenticated administrative web pages.

Trustwave Advisory: TWSL2020-011: Multiple Vulnerabilities in D-Link DSL-2888A (/en-us/resources/security-resources/security-advisories/?fid=28241)

Related SpiderLabs Blogs

(/en-us/resources/blogs/spiderlabs-blog/meta-phish-facebook-infrastructure-used-in-phishing-attack-chain/)

Meta-Phish: Facebook Infrastructure Used in Phishing Attack Chain (/en-us/resources/blogs/spiderlabs-blog/meta-phish-facebook-infrastructure-used-in-

SPIDERLABS BLOG

(/en-us/resources/blogs/spiderlabs-blog/trustwave-action-response-zero-day-vulnerability-in-citrix-adc-cve-2022-27518/)

Trustwave Action Response: Zero-Day Vulnerability in Citrix ADC (CVE-2022-27518) (/en-us/resources/blogs/spiderlabs-blog/trustwave-action-

SPIDERLABS BLOG

(/en-us/resources/blogs/spiderlabs-blog/going-mobile-bec-attacks-are-moving-beyond-email/)

Going Mobile: BEC Attacks Are Moving Beyond Email (/en-us/resources/blogs/spiderlabs-blog/going-mobile-bec-attacks-are-moving-beyond-

SPIDERLABS BLOG

(/en-us/resources/blogs/spiderlabs-blog/meta-phish-facebook-infrastructure-used-in-phishing-attack-chain/)

Meta-Phish: Facebook Infrastructure Used in Phishing Attack Chain (/en-us/resources/blogs/spiderlabs-blog/meta-phish-facebook-infrastructure-used-in-

SPIDERLABS BLOG

(/en-us/r
blog/trus
vulnerabi
27518/)

Trust
Zero-
Citrix
(/en-
us/re
blog/

SPIDERL

Stay Informed

Sign up to receive the latest security news and trends from Trustwave.

Business Email

SUBSCRIBE

English

(https://www.linkedin.com/company/trustwave)

(https://twitter.com/Trustwave)

(https://www.facebook.com/Trustwave/)

(https://www.youtube.com/channel/UC2CCqdrAxFv83NOdjhqA)

Leadership Team (/en-us/company/about-us/leadership/)

Our History (/en-us/company/about-us/our-history/)

News Releases (/en-us/company/newsroom/news/)

Media Coverage (/en-us/company/newsroom/media/)

Careers (https://jobs.jobvite.com/trustwave)

Global Locations (/en-us/company/global-locations/)

Awards & Accolades (/en-us/company/about-us/accolades/)

Trials & Evaluations (/en-us/resources/security-resources/special-offers/)

Contact (/en-us/company/contact/)

Support (/en-us/company/support/)

Security Advisories (/en-us/resources/security-resources/security-advisories/)

Software Updates (/en-us/resources/security-resources/software-updates/)