

[Try Akamai](#)[Under Attack?](#)[Products](#)[Resources](#)[Login](#)[Sales](#)[Akamai Products](#)[Customer Support](#)[I'm under attack and I need help](#)

Powered by Qualified
[Privacy Policy](#)

[Blog](#)

Command Injection on a



Assaf Vilmovski

February 09, 2021

Share



Your cookie choices for this website

We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie choices. Some cookies process personal data or personal information, where applicable. By continuing to visit our websites you are agreeing to our use of cookies and to the related processing activities. Click "Manage Preferences" to make individual choices and get details on the cookies in use and the processing activities in the Cookie Details section. You can access the Cookie Management Page and withdraw the consent at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)

[Manage Preferences](#)

reach all the floors. The goal was to have full connectivity from every location in the house.

As excited as I was to deploy the device and extend my network, eventually we decided to keep the top floor WiFi free, and I was left with a spare router. I decided to dive into some research on the device.

Starting off

To connect to its default access point (AP), you need to type the hardcoded token listed on the bottom of the device, as well as the user name, password, and the gateway address into the device's web interface. Once loaded, I started to browse the user interface. It looked like many other D-LINK products related to home networks, so I was in comfortable territory.

DAP-1360 - overview

The D-Link DAP-1360, according to the company's documentation, can "provide your wired network with wireless connectivity or upgrade your existing wireless network and extend its coverage."

The vulnerability I discovered was found in H/W Ver. A1, F/W Ver. 2.5.5, within the ping functionality of the web interface

Your cookie choices for this website

We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie choices. Some cookies process personal data or personal information, where applicable. By continuing to visit our websites you are agreeing to our use of cookies and to the related processing activities. Click "Manage Preferences" to make individual choices and get details on the cookies in use and the processing activities in the Cookie Details section. You can access the Cookie Management Page and withdraw the consent at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)

[Manage Preferences](#)

required in order for the OS (script or listener) to respect the request.

For example:

GET

```
/index.cgi?  
v2=y&proxy=y&rq=y&res_json=y&res_data_type=json&res_config_a  
ction=3&res_config_id=18&res_buf={%22host%22:  
%22192.168.0.5%22,%22count%22:1}  
&res_struct_size=0&res_pos=-1&tokenget=1268&&_=1593893639702  
HTTP/1.1
```

Host: 192.168.0.5

I see the position of the parameter inside the payload. With that information, I turned to Burp Suite, a collection of security tools used for vulnerability assessments and penetration testing.

Within Burp Suite, I positioned the `$p1val$` around the index of the IP and loaded it with payloads.

I used several known CMDi lists from [PayloadsAllTheThings](#).

Fortunately, the device did not ban me after multiple attempts, so I managed to find a format that responds with a valid status and retrieves a valid payload. To do this quickly, I had set special regex to extract the data from the response so it would appear in the main results window, instead of opening each response separately.

Your cookie choices for this website

We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie choices. Some cookies process personal data or personal information, where applicable. By continuing to visit our websites you are agreeing to our use of cookies and to the related processing activities. Click "Manage Preferences" to make individual choices and get details on the cookies in use and the processing activities in the Cookie Details section. You can access the Cookie Management Page and withdraw the consent at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)

[Manage Preferences](#)

How a malicious request looks

```
GET /index.cgi?
v2=y&proxy=y&rq=y&res_json=y&res_data_type=json&res_config_a
ction=3&res_config_id=18&res_buf={%22host%22:
%22192.168.0.52%7c%20ls%20-l%22,%22count%22:1}
&res_struct_size=0&res_pos=-1&tokenget=1268&&_=1593893639702
HTTP/1.1
```

Host: 192.168.0.52

Implications

Because the utility of the D-Link router will accept any command, an attacker can view, edit, or create any folder or file on the device. This opens the door to a number of attacks.

Let's say I login as "user" and the permissions on this account mean I can browse and manage the device, but I'm unable to login to the filesystem. In this example, the ping utility is in the OS and runs under a higher privileged account when compared to 'user'. This is a simple example of privilege escalation.

In the same scenario, a malicious user would be able to implement a persistent backdoor, allowing them to access the machine, with a higher privileged user on a regular basis, hidden from the conventional traffic logged by the device.

Your cookie choices for this website

We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie choices. Some cookies process personal data or personal information, where applicable. By continuing to visit our websites you are agreeing to our use of cookies and to the related processing activities. Click "Manage Preferences" to make individual choices and get details on the cookies in use and the processing activities in the Cookie Details section. You can access the Cookie Management Page and withdraw the consent at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)

[Manage Preferences](#)

4/07/2020: Report to d-link

5/07/2020: D-link security team response - waiting for their verification

15/07/2020: D-link confirms CMDi, providing a firmware for me to test the fix

18/07/2020: Tested the latest provided firmware, the vulnerability does no longer exist.

06/10/2020: [CVE-2020-26582](#) assigned

DLINK's Confirmation:

[D-link confirmation](#)

SITR

Share    



Written by
Assaf Vilmovski


Assaf Vilmovski is a Security Researcher at Akamai.

Related Blog Posts

Your cookie choices for this website

We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie choices. Some cookies process personal data or personal information, where applicable. By continuing to visit our websites you are agreeing to our use of cookies and to the related processing activities. Click "Manage Preferences" to make individual choices and get details on the cookies in use and the processing activities in the Cookie Details section. You can access the Cookie Management Page and withdraw the consent at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)

[Manage Preferences](#)



We're excited to launch AI Pulse, a blog series that takes a look at the current state of AI bots.

SECURITY

AI Pulse: OpenAI's Wild Bot Behavior After GPT-5

October 10, 2025

The AI Pulse series breaks down traffic trends and what they mean for apps, APIs, and businesses. In this post, read how OpenAI's bots are changing after GPT-5.

by Rob Lester

Your cookie choices for this website

We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie choices. Some cookies process personal data or personal information, where applicable. By continuing to visit our websites you are agreeing to our use of cookies and to the related processing activities. Click "Manage Preferences" to make individual choices and get details on the cookies in use and the processing activities in the Cookie Details section. You can access the Cookie Management Page and withdraw the consent at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)

[Manage Preferences](#)



October 08, 2025

Akamai was recognized as a Gartner Peer Insights Customers' Choice for WAAP for the sixth time. Discover why.

by Danielle Walter



We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie choices. Some cookies process personal data or personal information, where applicable. By continuing to visit our websites you are agreeing to our use of cookies and to the related processing activities. Click “Manage Preferences” to make individual choices and get details on the cookies in use and the processing activities in the Cookie Details section. You can access the Cookie Management Page and withdraw the consent at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)

Manage Preferences

Explore how post-quantum cryptography standards vary by country, which algorithms are approved globally, and how to guard against future quantum threats.

by Jan Schaumann

[Read more >](#)

Rate the helpfulness of this page



Your cookie choices for this website

We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie choices. Some cookies process personal data or personal information, where applicable. By continuing to visit our websites you are agreeing to our use of cookies and to the related processing activities. Click "Manage Preferences" to make individual choices and get details on the cookies in use and the processing activities in the Cookie Details section. You can access the Cookie Management Page and withdraw the consent at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)

[Manage Preferences](#)

[History](#)[Leadership](#)[Facts and Figures](#)[Awards](#)[Board of Directors](#)[Investor Relations](#)[Corporate Responsibility](#)[Ethics](#)[Locations](#)[Vulnerability Reporting](#)

CAREERS

[Careers](#)[Working at Akamai](#)[Students and Recent Grads](#)[Workplace Diversity](#)[Search Jobs](#)[Culture Blog](#)

NEWSROOM

[Newsroom](#)[Press Releases](#)[In the News](#)[Media Kit](#)

Your cookie choices for this website

We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie choices. Some cookies process personal data or personal information, where applicable. By continuing to visit our websites you are agreeing to our use of cookies and to the related processing activities. Click "Manage Preferences" to make individual choices and get details on the cookies in use and the processing activities in the Cookie Details section. You can access the Cookie Management Page and withdraw the consent at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)

[Manage Preferences](#)

What Is Cloud Computing?

What Is Cybersecurity?

What Is a DDoS attack?

What Is Microsegmentation?

What Is WAAP?

What Is Zero Trust?

[See all](#)



[EMEA Legal Notice](#)

[Service Status](#)

[Contact Us](#)

[🌐 EN ©2025 Akamai Technologies](#)

Your cookie choices for this website

We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie choices. Some cookies process personal data or personal information, where applicable. By continuing to visit our websites you are agreeing to our use of cookies and to the related processing activities. Click “Manage Preferences” to make individual choices and get details on the cookies in use and the processing activities in the Cookie Details section. You can access the Cookie Management Page and withdraw the consent at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)

[Manage Preferences](#)