< Back to all zero days

D-Link Router DIR-868L Telnet Hardcoded credentials

AFFECTED VENDOR
D-Link

STATUS
Fixed

DATE
Aug 18, 2020

Description Proof of concept (POC) Impact Remediations Timeline

Description

The D-Link router DIR-868L 3.01 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.

Proof of concept: (POC)

Issues:

The telnet hardcoded default credentials are the vulnerable elements in the firmware of DIR-868L.

Step 1: Extract the firmware

Step 2: Run the command cat etc/init0.d/S80telnetd.sh to get the username and the location of the variable used for storing the password.

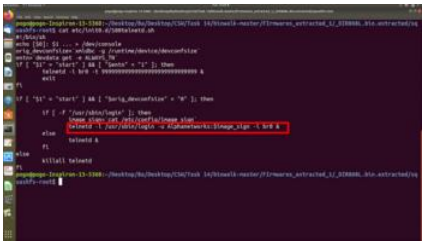

Figure 1: *Clear text username as shown in screenshots*

Step 3: Run the command cat etc/config/image_sign to get the password

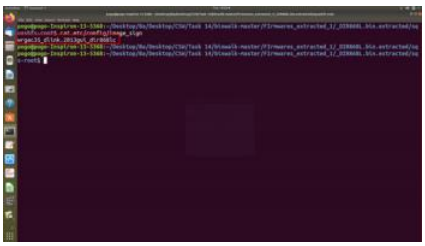

Figure 2: *Clear text password as shown in screenshots*

Impact

A successful exploit could allow the attacker to gain access to the firmware and to extract sensitive data.

Remediations

D-Link released a support announcement in response to the recommendations provided by CSW team for these D-Link products
- https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10189

Timeline

Aug 17, 2020: Discovered in our research lab

Aug 18, 2020: Vulnerability reported to vendor and vendor acknowledged the vulnerability

Aug 20, 2020: Vendor responded saying "elevated to D-Link Corporation".

Aug 26, 2020: Follow up

Aug 28, 2020: Vendor responded saying "should have an update in next few Days"

Sep 4, 2020: Follow up

Sep 7,2020: Vendor responded saying need more time to review and response from R&D

Sep 10, 2020: Vendor responded with a support announcement.

Discovered by

Cyber Security Works Pvt. Ltd.

Advisory

Affected Vendor
D-Link

Bug Name
Telnet Hardcoded credentials

CVE Number
CVE-2020-29321

CWE ID
CWE - 798

CSW ID
2020-CSW-08-1046

CVSSv3 Score
8.1

Affected Version
3.01

Severity
High

Affected Product
D-Link

Talk to CSW's team of experts to secure your landscape.

Schedule free consultation

Cyber Security Works helps reduce security debt and inherent vulnerabilities in an organization's infrastructure and code. We work with large public, private, and start-up companies and help them prioritize their vulnerabilities.

Resources

- Ransomware
- Cyber Risk Series
- Blogs
- Patch Watch
- Data Sheets
- White Papers
- Zero Days
- Glossary
- Events
- CISA-KEV

Partner

- Become a Partner

Quick Links

- About Us
- Contact Us
- Careers
- Services
- Media Coverage
- Cybersecurity month
- Predictions for 2022
- Cybersecurity for govt
- Hackathon