D-Link DIR-615 Router Multiple Vulnerabilities

SYNOPSIS:

D-Link DIR-615 series router suffers from Multiple Cross-Site-Request-Forgery, Sensitive Information Disclosure and Weak IP Based Session Management Vulnerabilities.


CVE:

- [http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7404](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7404)
- [http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7405](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7405)
- [http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7406](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7406)

VULNERABILITY DETAILS:

Lab Setup:

1. Target Router: DIR-615 Router (Hardware Version: T1, Firmware Version: 20.12PTb01)
2. Target IP Address: 192.168.100.1
3. Malicious Site: [http://139.XX.XX.XXX](http://139.XX.XX.XXX)

Vulnerable/Tested Version:

DIR-615 running latest firmware version 20.12PTb01 is affected. Other models may also be affected.
Vulnerability #1: Cross Site Request Forgery Vulnerability on Firmware Upgrade Page

The device does not protect following sensitive page from CSRF attack:


An unauthenticated, remote attacker could host a malicious website that either sends a POST request to Firmware Upgrade Page.

**Risk Factor:** High

**Impact:**

If a victim is logged in to the Router’s Web Interface and visits a malicious site from another tab in the same browser, the malicious site then can send requests to the victims Router without knowing the credentials.

An attacker can host a page which sends POST request to Form2File.htm that tries to upload Firmware to victim’s Router. This causes router to reboot/crash resulting into Denial of Service. An attacker may succeed in uploading a malicious Firmware if he plays little bit around this.

**Proof-Of-Concept: CSRF on Firmware Upgrade Page**

**CVSS Score:** AV: N/AC: M/AU: N/CI: N/A:C

1. Capture Firmware update request in BurpSuite Pro.

2. Generate CSRF-PoC using BurpSuite Pro
Note: Make sure to select Options->CSRF Technique->Plain Text Form and Options->CSRF Technique->Include auto-submit script options

3. Copy this HTML and save it as **Burp-CSRF.html** under web root on Kali machine.
   Note: I’ve already hosted it on malicious site **http://139.XX.XX.XXX/Burp-CSRF.html**

4. Victim logs into Router’s Web Interface.

5. Victim visits **http://139.XX.XX.XXX/Burp-CSRF.html**

**Note:** Victim doesn’t have to click ‘Submit Request’ button as the option ‘Include auto-submit script’ was used while generating CSRF POC using BurpSuite. This submits the form automatically on page load.
Router resets the connection.

Request in BurpSuite:

Victim visits malicious page
Malicious page sends Firmware upload request to victim's router
Router is now inaccessible. Also, the Wireless LAN icon in the System Tray indicates that it has connectivity issues:
Vulnerability#2: IP Based Weak Session Management

Once user is authenticated, this device keeps track of user’s session by using the IP address of his machine. An internal attacker could sniff the network traffic to find out if victim is logged into the router.

Risk Factor: **High**

**Impact:**

Once authenticated, this device identifies the user based on the source IP address of the victim's host. By spoofing the IP address belonging to the victim's host, an attacker might be able to take over the administrative session without being prompted for authentication credentials. An attacker can get victim’s and router's IP address by simply sniffing the network traffic.

**Proof-Of-Concept:**

**CVSS Score:** AV: N/AC: M/AU: N/C: N/I: C/A:C

1. Launch Internet Explorer and log into the router’s web interface
2. Now launch Firefox and access http://192.168.100.1/wlan_basic.htm

It doesn’t prompt for password. Looking at the request in BurpSuite, it’s not using any Cookie or HTTP Basic/Digest authentication for session management.

GET /wlan_basic.htm HTTP/1.1
Host: 192.168.100.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.1/status.htm
Cookie: SessionID=
Connection: close
Upgrade-Insecure-Requests: 1

Also, highlighted is the Pre-Shared Key received in response.
An attacker can simply spoof victim’s IP address and take over the victim’s session. Moreover, if victim has web access enabled on his router and is accessing the web interface from different network which is behind the NAT/Proxy, an attacker can sniff the network traffic to know the public IP address of the victim’s router and take over his session as he won’t be prompted for credentials.
Vulnerability#3: Sensitive Information Disclosure

This device doesn’t use SSL for any of the authenticated pages. Also, it doesn't allow user to generate his own SSL Certificate. An attacker can simply monitor network traffic (like an open wireless network), and steal user’s credentials and/or credentials of users being added while sniffing the traffic.

**Risk Factor:** High

**Impact:**

An attacker can steal user’s credentials to access router’s web interface, thus compromising Confidentiality, Integrity and Availability

**Proof-Of-Concept:**

**CVSS Score:** AV: N/AC: L/AU: N/C: N/I: C/A:C

1. Log into the router’s web interface.
2. Credentials submitted in plain text
CREDITS:
The discovery and documentation of this vulnerability was conducted by Kapil Khot, Qualys Vulnerability Signature/Research Team.

CONTACT:
For more information about the Qualys Security Research Team, visit our website at http://www.qualys.com or send email to research@qualys.com

LEGAL NOTICE:
The information contained within this advisory is Copyright (C) 2017 Qualys Inc. It may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way.