Computest
always on.

Afstudeeronderzoek **Security**

Afstudeeronderzoek van Timo Musters
D-Link camera’s

INTRO

Tijdens mijn afstudeeronderzoek bij Computest naar kwetsbaarheden in IP-camera’s stuitte ik op het merk D-Link. Dit is een Taiwanese fabrikant van producten voor netwerken, draadloze verbindingen, breedband, digitale elektronica, spraak en datacommunicatie en IoT-apparaten. Deze camera’s zijn relatief veilig wanneer de software up-to-date is en de camera’s op de juiste manier worden geconfigureerd. Uit mijn onderzoek is gebleken dat dit niet altijd het geval is.

1. Kwetsbaarheden en firmwareupdates in D-Link IP-camera's

Tijdens mijn afstudeeronderzoek bij Computest naar kwetsbaarheden in IP-camera's stuitte ik op het merk D-Link. Dit is een Taiwanese fabrikant van producten voor netwerken, draadloze verbindingen, breedband, digitale elektronica, spraak- en datacommunicatie en IoT-apparaten. Deze camera's zijn relatief veilig wanneer de software up-to-date is en de camera's op de juiste manier worden geconfigureerd. Uit mijn onderzoek is gebleken dat dit niet altijd het geval is. De camera's van D-Link die ik heb onderzocht zijn allemaal nog kwetsbaar voor de reeds bekende kwetsbaarheid CVE-2018-18441.
Bron: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18441

Deze kwetsbaarheid stelt een aanvaller die zich op hetzelfde netwerk als de IP-camera bevindt in staat om op afstand gevoelige gegevens als de productnaam, leverancier, model, firmwareversie, IP-adres, MAC-adres en meer uit te lezen. Met al deze bemachtigde gegevens kan er gericht worden gezocht op bekende kwetsbaarheden in de IP-camera.

Normaal gesproken is dit eenvoudig te verhelpen met een update van de fabrikant, maar bij de D-Link camera's zit een probleem in het bijwerken van de software.

1.1. Het (omslachtige) updateproces

De software van de IP-camera's die ik onderzocht heb kan worden bijgewerkt via een lokale webpagina op het apparaat zelf. Deze webpagina ziet er als volgt uit:

Op deze website biedt de fabrikant niet de optie om automatisch de nieuwste firmware te downloaden, maar biedt de fabrikant een link naar een download pagina waar nieuwe firmware te downloaden is. Wanneer de gebruiker op de link klikt komt hij niet direct op een download pagina, maar gewoon op de website http://www.dlink.com, de website van de fabrikant. Hier moet de gebruiker vervolgens zelf door de site gaan zoeken naar updates, wat een zeer omslachtig proces blijkt. Tevens is de website niet bijgewerkt waardoor er niet voor ieder model de juist updates staan. Updaten lijkt haast onmogelijk.

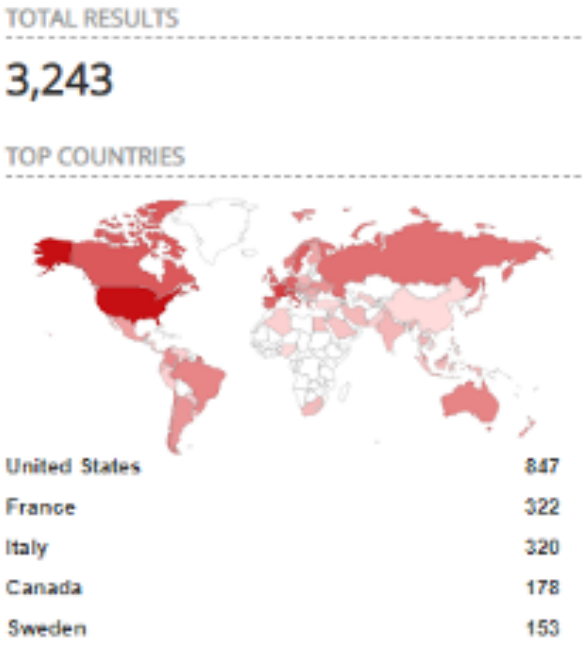
Na verder onderzoek blijkt het dat D-Link op meerdere manieren probeert updates te pushen naar haar gebruikers. Dit zijn de drie manieren:

- Via een mobiele app, maar deze geeft geen updatefunctie als je de camera zonder account gebruikt.
- Via de omslachtige D-Link website, die een gebruiker zelf moet doorzoeken.
  https://eu.dlink.com/nl/nl/products/dcs-932l-day-night-cloud-camera?revision=deu_revb#downloads
  Echter, deze website biedt enkel oude firmwareversies 2.17.01.
- Na verder zoeken kun je via de US-website van D-Link wel meer informatie halen als consument en daar staat wel de juiste update klaar namelijk versie 2.18.01.
  https://support.dlink.com/ProductInfo.aspx?m=DCS-932L

1.2. Over hoeveel IP-camera's hebben we het eigenlijk?

Doordat de D-Link IP-camera's niet automatisch of semi-automatisch updaten moet de gebruiker een omslachtig proces doorlopen voordat zijn camera wordt bijgewerkt naar de meest recente firmwareversie. Dit proces zal ook iedere keer als er een nieuwe update is doorlopen moeten worden. Een klein onderzoekje naar de aanwezigheid op het internet van IP-camera's van het model DCS-932 toont in maart 2020 zo'n **3,243 apparaten**.

Voor dit onderzoek is de zoekmachine shodan.io gebruikt, een zoekmachine waarmee apparaten op het internet doorzocht kunnen worden op bepaalde eigenschappen zoals model naam poort en land. De zoekopdracht die hierboven gebruikt is ziet er als volgt uit: https://beta.shodan.io/search?query=dcs-932l



Nu zullen niet alle camera's verouderde software bevatten, maar ik vermoed dat het zeker bij meer van de helft van de IP-camera's het geval is. Bovenstaand getal is alleen nog maar het aantal IP-camera's op het internet van het model DCS-932. Laat staan alle andere modellen van D-Link: **DCS-936L, DCS-942L, DCS-8000LH, DCS-942LB1, DCS-5222L, DCS-825L, DCS-2630L, DCS-820L, DCS-855L, DCS-2121, DCS-5222LB1, DCS-5020L, en de vele anderen**.

1.3. Voorbeelden uit Nederland

Als voorbeeld heb ik een aantal camera's onderzocht die vanuit Nederland aan het internet zijn gehangen. In totaal zijn er volgens shodan.io 46 camera's in Nederland. Hiervan heb ik de eerste 4 nader onderzocht om de exacte firmwareversie te kunnen bepalen.

4 voorbeelden van de 46 IP-camera's in Nederland met model dcs-932L			
Model	**Firmware**	**Nieuwste/firmware**	**goed/verouderd**
DCS-932L-A	1.10	1.14.04	Verouderd
DCS-932L	1.06	1.14.04	Verouderd
DCS-932L-A	1.04	1.14.04	Verouderd
DCS-932L	1.12	1.14.04	Verouderd

Mijn vermoeden wordt bevestigd; alle onderzochte camera's draaien op een verouderde firmwareversie.

1.4. In hoeverre kunnen kwetsbaarheden in verouderde software ook echt misbruikt worden?

Voor het model DCS-923L dat ik heb onderzocht zijn er 3 CVE's (publiek bekende kwetsbaarheden) gemeld. Als de gebruiker de camera netjes bijwerkt naar de laatste versie zullen deze CVE's niet van toepassing zijn, alleen dit is dus niet altijd mogelijk of gemakkelijk. De camera's die ik via shodan.io bekeken heb blijken vatbaar voor 2 van de 3 bekende kwetsbaarheden, namelijk namelijk CVE-2019-10999 en CVE-2017-7852.
Bron: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=DCS-932l

CVE-2019-10999 stelt een geauthenticeerde aanvaller op afstand in staat om de camera tijdelijk buiten werking te stellen. Hierdoor kan de consument de webpagina van de camera niet meer bereiken en kan de app op de smartphone van de consument geen verbinding meer leggen met de IP-camera. De enige randvoorwaarde is dat een aanvaller beschikt over een valide account op de IP-camera, maar veel consumenten wijzigen de standaard accountgegevens niet.

De tweede kwetsbaarheid met **CVE-2017-7852** gaat over de aanwezigheid van een onvoldoende veilig cross-domain policy voor Flash. Een aanvaller kan deze kwetsbaarheid misbruiken door een ingelogde IP-camera gebruiker te lokken naar een kwaadaardige website, waar automatisch via een Flash-filmpje acties worden uitgevoerd binnen de webomgeving van de IP-camera. Hiermee kan een aanvaller bijvoorbeeld de instellingen van de camera veranderen of een admin gebruiker toevoegen, zonder dat het slachtoffer dit door heeft.

1.5. Wat nu?

Een degelijk, veilig IoT product heeft de mogelijkheid om op een automatische manier software updates door te kunnen voeren. D-Link heeft het helaas niet zo goed voor elkaar en heeft het camera-eigenaren flink lastig gemaakt om hun software bij te werken naar de meest recente versie.

De eerste stap in het veilig gebruik van een IP-camera is om deze NOOIT direct aan het internet te hangen. Dit opent de mogelijkheid voor aanvallers om de camera te vinden en vervolgens aan te vallen.

Daarnaast blijft updaten de enige oplossing. Omdat dit niet makkelijk wordt gemaakt, beschrijf ik hieronder twee manieren om uw camera up-to-date te brengen en te houden.

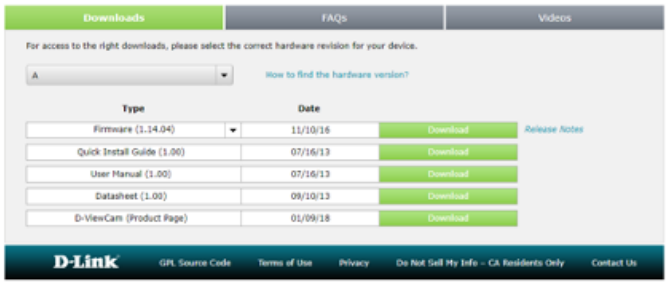
Manier 1: de website van D-Link

Ga naar de website https://support.dlink.com/

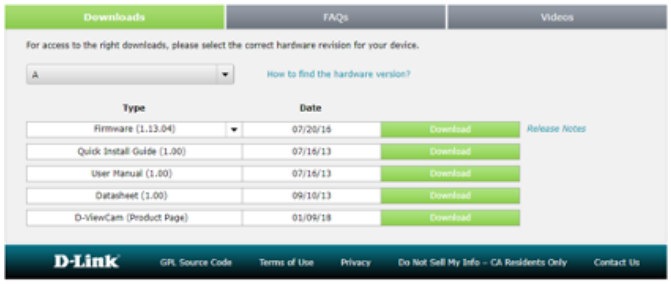
In de zoekbalk van de website zoek je naar het model van de camera. Aan de achterkant of onderkant van de camera zit een sticker waarop staat welk model het is.

Als voorbeeld neem ik de DCS-932L. Wanneer u op de correct pagina bent moet een selectie maken of u versie a of b heeft. Dit kunt u ook zien aan de achterkant van de camera. Mocht u een ander model D-Link camera bezitten dan kan het zijn dat u de versie a of b stap kunt overslaan.

Vervolgens selecteert u de nieuwste firmware, deze is standaard geselecteerd maar u kunt het ook nog verifiëren met de datum die u links ziet. Klik op 'Download' om het firmwarebestand te downloaden.



Figuur 1 nieuwste update.
Dit kun je zien aan de datum *date

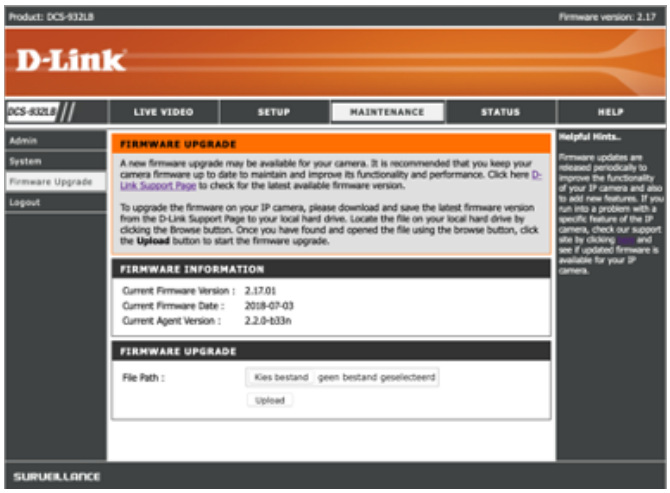


Figuur 2 oudere update niet goed.
Dit kun je zien aan de datum *date =verouderd

Vervolgens dient u in te loggen op het portaal van uw camera. Dit portaal kunt u vinden door het IP-adres van uw IP-camera te bezoeken met uw browser, bijvoorbeeld http://<ip.adres>:80

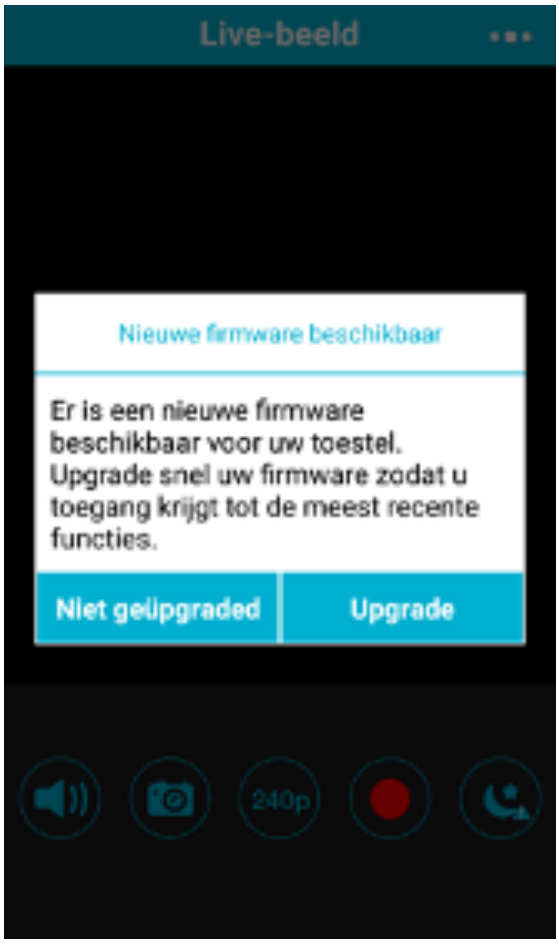
Kies in het menu Maintenance voor Firmware Upgrade.

Wanneer u op deze pagina bent gaat u naar 'Kies bestand' en selecteert u het bestand dat u paar stappen terug gedownload heeft en kiest u voor 'Upload'. Nu moet u een moment geduld hebben en zal uw camera worden bijgewerkt naar de laatste versie. Dit kunt u controleren door naar 'Current Firmware Version' te kijken in het openstaande scherm.



1.5.2 Manier 2: de mydlink mobiele app

D-Link levert bij de IP-camera's ook een mobiele app genaamd mydlink. Hiermee kan de consument ook zijn of haar camera's updaten. Dit is alleen mogelijk wanneer u een account heeft aangemaakt; u moet uzelf dus wel registreren anders krijgt u geen updates. Wanneer u een account heeft aangemaakt krijgt u direct de onderstaande melding:



Mocht u deze melding niet zien, ga dan naar de 3 bolletjes aan de linker bovenkant van de app.

Vervolgens ziet u firmware bijwerken en volgt u de stappen in de opvolgende schermen. Hierna zal de camera alsnog geüpdatet worden.