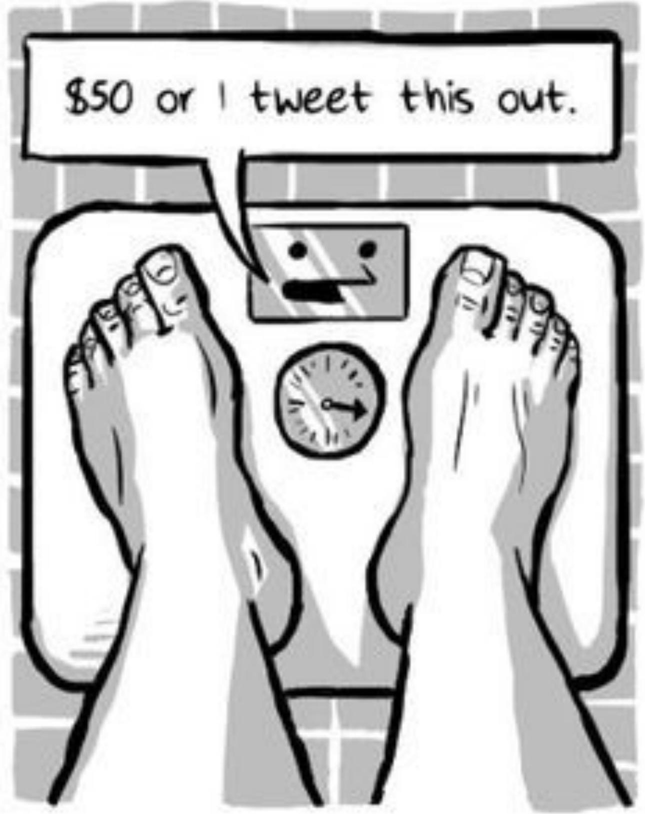


IoT Security: My Worst Nightmares Come True and How To Sleep Better At Night

Paul Asadoorian

Security Weekly, Founder & CEO

Offensive Countermeasures, CEO

About Me

- I run the Security Weekly podcast network
- I am the CEO at Offensive Countermeasures
- I've worked building security infrastructure, penetration testing and as a product specialist for Tenable Network Security
- I studied Kung Fu for about 10 years (Long Fist AKA Changquan and Tai Chi)
- I've watched A LOT of Kung Fu movies (500+)

DISCLAIMER

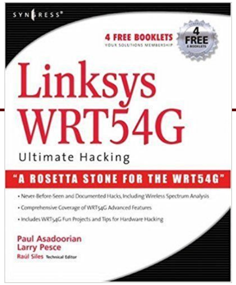
“The opinions, words, phrases, sentences, so-called facts, images, and/or videos expressed in this presentation and on the following slides are solely those of the presenter and not necessarily those of his employer, the conference, sponsors, affiliates, security vendors, or anyone else. Only Paul could guarantee the accuracy or reliability of the information provided herein (but does not anyhow).

If you are easily offended by imagery, puns, jokes, funny phrases, adult language and humor, or anything even close to the above, please excuse yourself from this presentation.”

Talk Outline

- How did I come up with this talk?
- Part 1: My IoT Nightmares Come True
- Part 2: Glimmers Of Hope for Iot Security

Flashback: 2007



SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

4 FREE E-BOOKLETS

Linksys WRT54G

Ultimate Hacking

"A ROSETTA STONE FOR THE WRT54G"

- Never-Before-Seen and Documented Hacks, Including Wireless Spectrum Analysis
- Comprehensive Coverage of WRT54G Advanced Features
- Includes WRT54G Fun Projects and Tips for Hardware Hacking

Paul Asadoorian
Larry Pesce
Raúl Siles Technical Editor

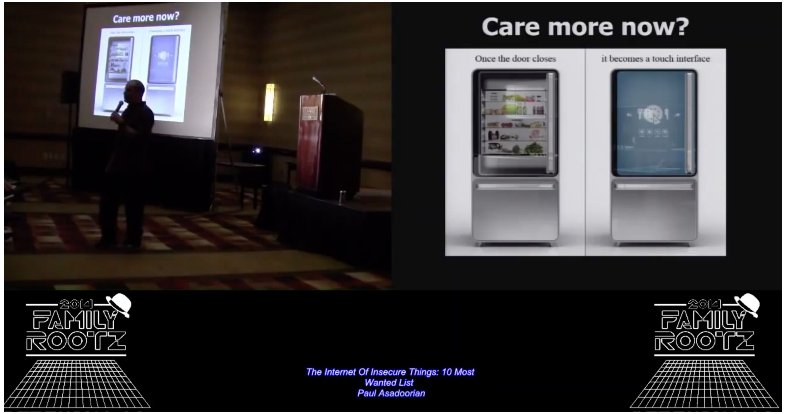
I realized after writing a book (and a course) that embedded security was getting worse, not better

I began focusing on Embedded Device Security, (now called IoT "security")

ACID FLASHBACKS

The origin of most today's children's shows

More Talks



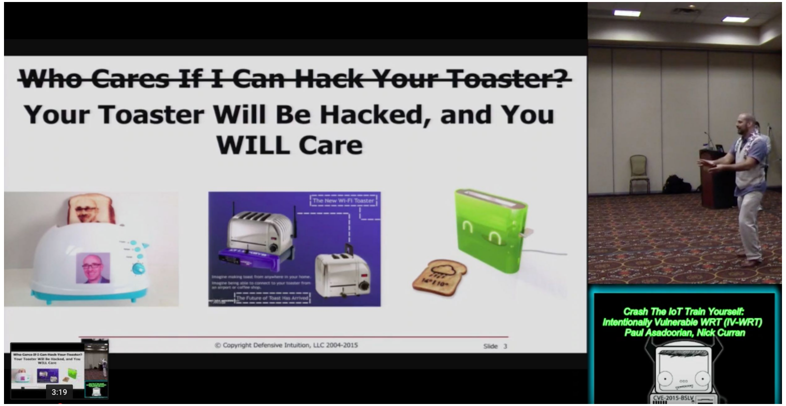
Care more now?

Once the door closes

it becomes a touch interface

The Internet Of Insecure Things: 10 Most Wanted List
Paul Asadoorian

I gave several talks on embedded device insecurity (You can find all of my materials here: http://wiki.securityweekly.com/wiki/index.php/EmbeddedDevices



~~Who Cares If I Can Hack Your Toaster?~~

Your Toaster Will Be Hacked, and You WILL Care

© Copyright Defensive Intuition, LLC 2004-2015 Slide 3

Crash The IoT Train Yourself: Intentionally Vulnerable WRT (IV-WRT)
Paul Asadoorian, Nick Curran

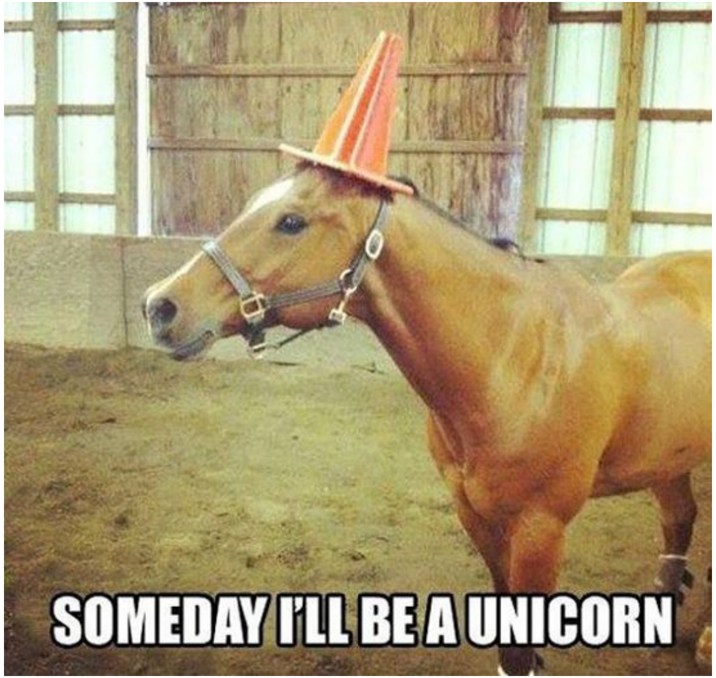
I communicated many theories on how devices could be hacked and used by bad guys

I even helped create vulnerable on-purpose firmware, an effort to raise awareness

I Gave Up

After years on the subject, I gave up

IoT devices were more ubiquitous, and just as vulnerable as ever



Realization

I realized all that stuff I dreamed about bad guys doing with IoT was coming true!

I also realized there were new initiatives to secure IoT, but they need support from our community

Hence this talk, Nightmares first, then stuff we can support to help...

Trying Not To Say "I Told You So"

"There's no reason the average user would ever think that their webcam—or more likely, a small business's—is potentially part of an active botnet. And even if it were, ***there's not much they could do about it, having no direct way to interface with the infected product.****"*

"The Botnet That Broke The Internet Isn't Going Away", Wired Magazine, December 2016

- Lily Hay Newman

https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

"First, there is typically not a monitor, mouse, keyboard, or end-user associated with a network device. Console connections are the closest thing, however typically they are used only when performing maintenance or to recover a device from a failure. ***The absence of a user interface makes it much easier to hide our presence.****"*

(IN)SECURE Magazine, ISSUE 14 (November, 2007)

- Paul Asadoorian

https://www.helpnetsecurity.com/dl/insecure/INSECURE-Mag-14.pdf

Nightmare #1

An IoT botnet would be created using multiple payloads for different processor architectures.

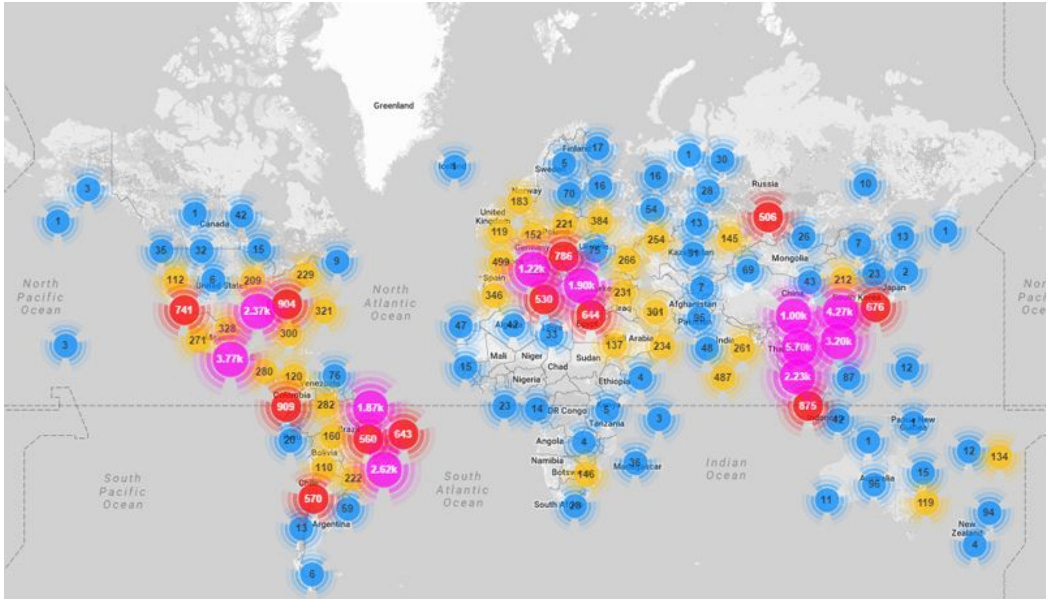
http://TheFunnyPlace.net

Mirai

49,657 unique IPs which hosted Mirai-infected devices

Mirai-infected devices were spotted in 164 countries

The attack peaked at 650 Gbps of traffic.

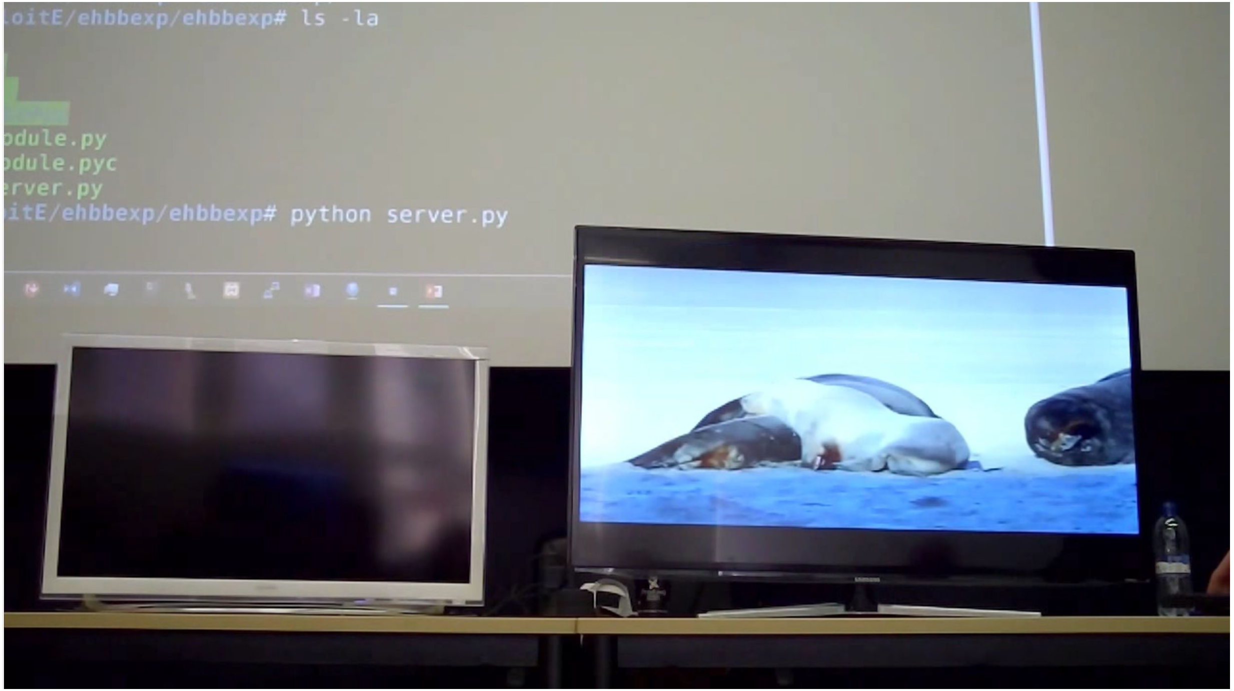


63 default credentials and 21 different payloads for various architectures, bonus: open-source!

Nightmare #2

IoT devices will be hacked, and used as a vehicle to serve unwanted and unauthorized ads

Hacking TVs Over-The-Air



```
oitE/ehbbexp/ehbbexp# ls -la

odule.py
odule.pyc
rver.py
itE/ehbbexp/ehbbexp# python server.py
```

DVB-T is used to gain remote shell to a TV over-the-air

You need to be in some physical proximity

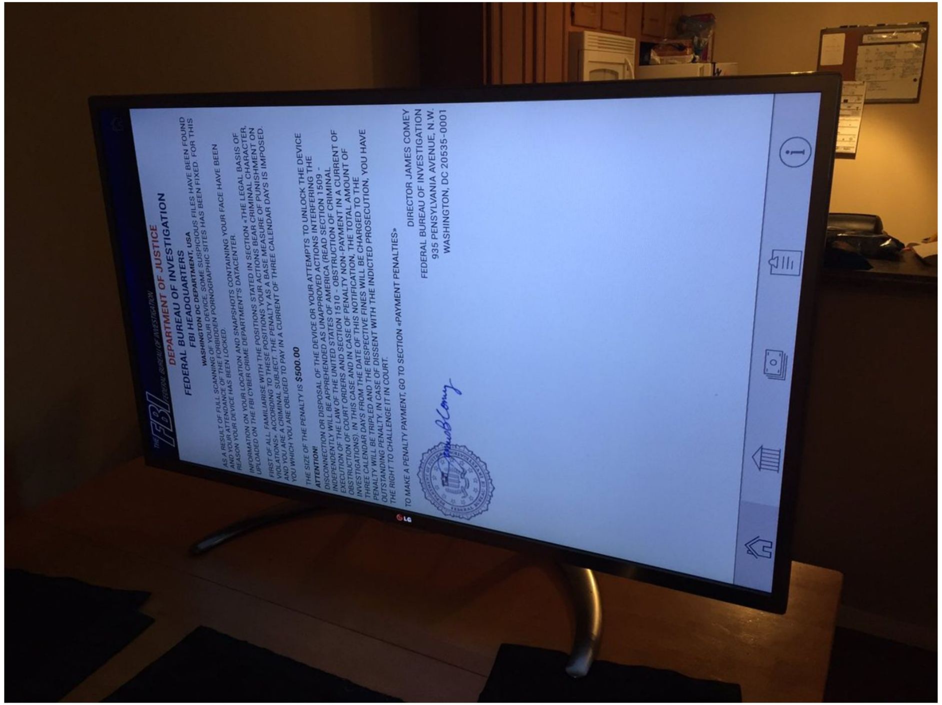
The TV’s can only phone home or attack other devices if they are connected to the network

Infections persisted over reboots and factory resets

You can put the transmitter on a drone….

https://arstechnica.com/security/2017/03/smart-tv-hack-embeds-attack-code-into-broadcast-signal-no-access-required/

TVs Infected With Ransomware



THE FBI FEDERAL BUREAU OF INVESTIGATION

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVERS
FBI HEADQUARTERS
WASHINGTON DC DEPARTMENT, USA

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION «THE LEGAL BASIS OF VIOLATIONS». ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED.

THE SIZE OF THE PENALTY IS **$500.00**

ATTENTION!
DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND SECTION 1510 - OBSTRUCTION OF CRIMINAL INVESTIGATIONS). IN THIS CASE AND IN CASE OF PENALTY NON-PAYMENT IN A CURRENT OF THREE CALENDAR DAYS FROM THE DATE OF THIS NOTIFICATION, THE TOTAL AMOUNT OF PENALTY WILL BE TRIPLED AND THE RESPECTIVE FINES WILL BE CHARGED TO THE OUTSTANDING PENALTY. IN CASE OF DISSENT WITH THE INDICTED PROSECUTION, YOU HAVE THE RIGHT TO CHALLENGE IT IN COURT.

TO MAKE A PENALTY PAYMENT, GO TO SECTION «PAYMENT PENALTIES»

DIRECTOR JAMES COMEY
FEDERAL BUREAU OF INVESTIGATION
935 PENSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20535-0001

LG smart TV infected with ransomware [Source: Darren Cauthon]

Low occurrence, one malware strain found to target TVs (Cyber.Police AKA FLocker)

Ransomware demands $500, and LG wants $340 for a service call

You can just buy a new TV, a $100 ransom might be worth it

LG did help, and now there is a YouTube video showing how to un-ransomware yourself (https://www.youtube.com/watch?v=0WZ4uLFTHEE)

https://www.bleepingcomputer.com/news/security/android-ransomware-infects-lg-smart-tv/

Nightmare #3

Consumers will continue not to care about the security of IoT devices.

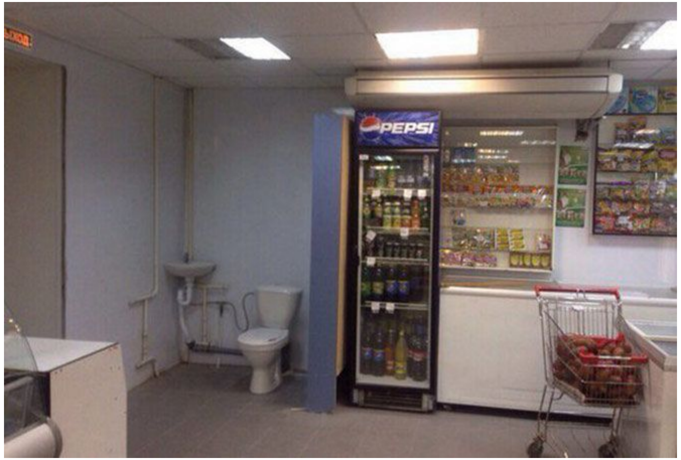
Worse: Buyers & Sellers!

The market can't fix this because neither the buyer nor the seller cares. *The owners of the webcams and DVRs used in the denial-of-service attacks don't care. Their devices were cheap to buy, they still work, and they don't know any of the victims of the attacks. The sellers of those devices don't care: They're now selling newer and better models, and the original buyers only cared about price and features. There is no market solution, because the insecurity is what economists call an externality: It's an effect of the purchasing decision that affects other people. Think of it kind of like invisible pollution.*

https://www.schneier.com/blog/archives/2017/02/security_and_th.html

Nightmare #4

Manufacturers will continue not to care about the security of IoT products.

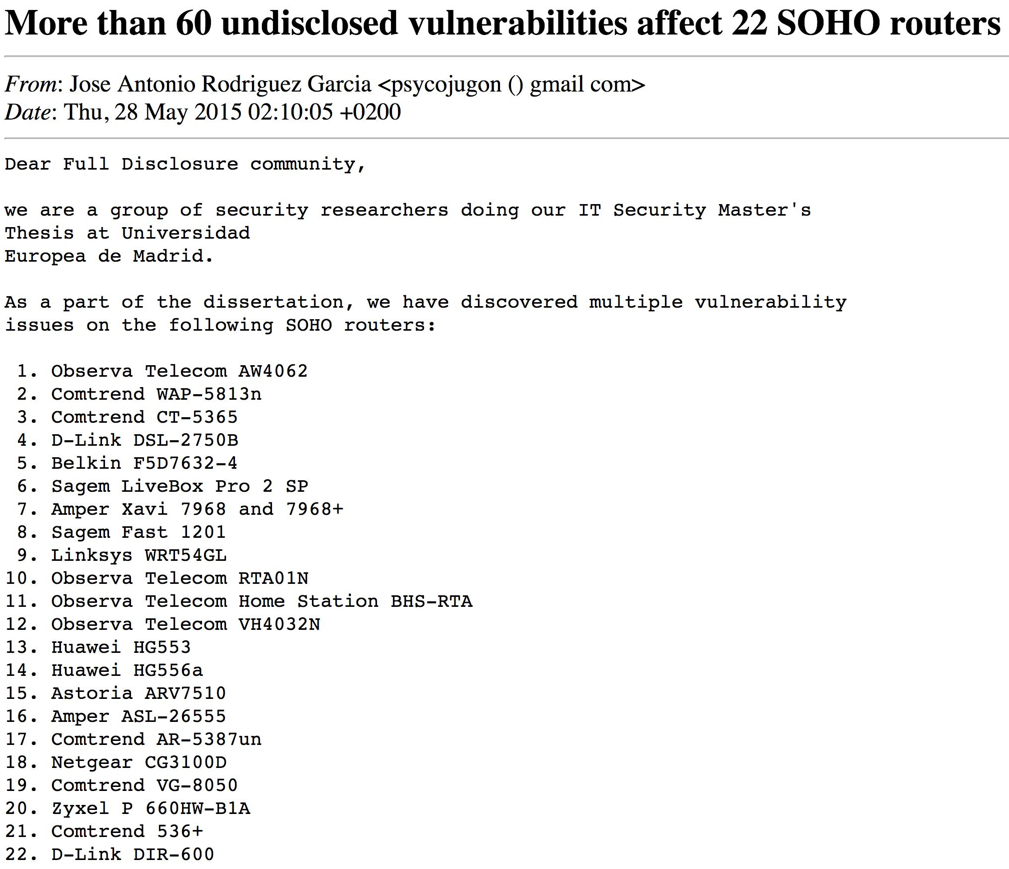


Numbers Matter

Vulnerabilities included:

- XSS
- Denial of Service (DoS)
- Authentication Bypass
- UPnP vulnerabilities

http://seclists.org/fulldisclosure/2015/May/129



More than 60 undisclosed vulnerabilities affect 22 SOHO routers

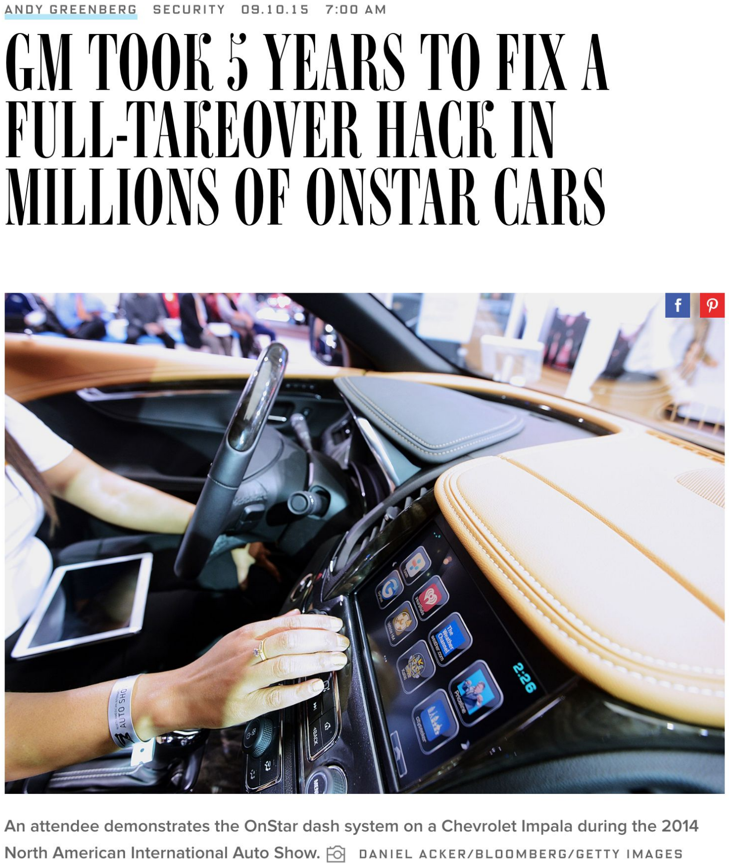
From: Jose Antonio Rodriguez Garcia <psycojugon () gmail com>
Date: Thu, 28 May 2015 02:10:05 +0200

Dear Full Disclosure community,

we are a group of security researchers doing our IT Security Master's
Thesis at Universidad
Europea de Madrid.

As a part of the dissertation, we have discovered multiple vulnerability
issues on the following SOHO routers:

1. Observa Telecom AW4062
2. Comtrend WAP-5813n
3. Comtrend CT-5365
4. D-Link DSL-2750B
5. Belkin F5D7632-4
6. Sagem LiveBox Pro 2 SP
7. Amper Xavi 7968 and 7968+
8. Sagem Fast 1201
9. Linksys WRT54GL
10. Observa Telecom RTA01N
11. Observa Telecom Home Station BHS-RTA
12. Observa Telecom VH4032N
13. Huawei HG553
14. Huawei HG556a
15. Astoria ARV7510
16. Amper ASL-26555
17. Comtrend AR-5387un
18. Netgear CG3100D
19. Comtrend VG-8050
20. Zyxel P 660HW-B1A
21. Comtrend 536+
22. D-Link DIR-600



ANDY GREENBERG SECURITY 09.10.15 7:00 AM

GM TOOK 5 YEARS TO FIX A FULL-TAKEOVER HACK IN MILLIONS OF ONSTAR CARS

An attendee demonstrates the OnStar dash system on a Chevrolet Impala during the 2014 North American International Auto Show. DANIEL ACKER/BLOOMBERG/GETTY IMAGES

https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/

Hacking Sex Toys

Supported By
Pornhub
The Internet Of Dongs Project
Hacking Sex Toys For Security And Privacy

Brad Haines (a.k.a. Render Man) on Internet of Dongs - Paul's Security Weekly #505

https://youtu.be/TDtEBMLxwLE

Many of the manufacturers have no clue about IT OR Security!

Very difficult disclosure process (typically, Pen Test Partners got it wrong) https://internetofdon.gs/2017/04/04/rebuttal-to-pen-test-partners/

Nightmare #5

IoT devices would grow in market share and new technologies would make them even more ubiquitous than ever before

“Alexa”

http://smarthome.reviewed.com/features/everything-that-works-with-amazon-echo-alexa

Nightmare #6

People will feel safe because they have a firewall to protect IoT devices from the Internet

Some Theory (And TV)

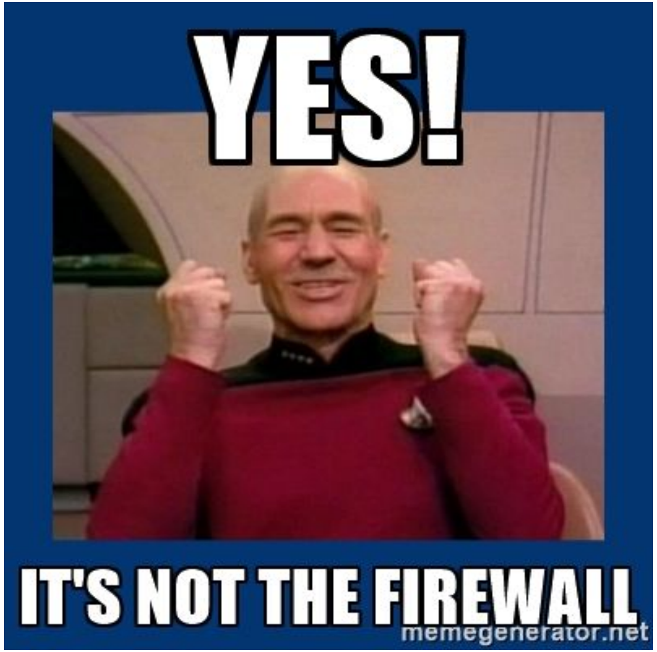
The research paper “Smartphones attacking smart homes” was presented at the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2016).

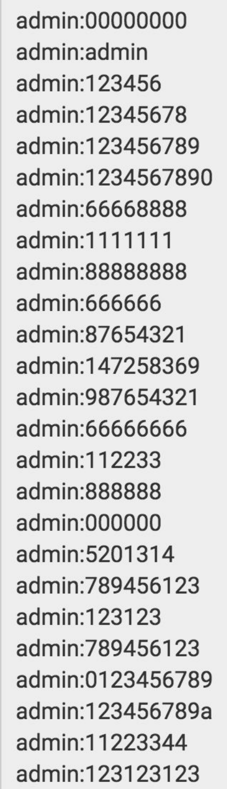
“In this paper we demonstrate how an attacker can infiltrate the home network via a doctored smart-phone app. Unbeknownst to the user, this app scouts for vulnerable IoT devices within the home, reports them to an external entity, and modifies the firewall to allow the external entity to directly attack the IoT device.”

http://dl.acm.org/citation.cfm?doid=2939918.2939925

Already Happening

"The trojan, dubbed Trojan.AndroidOS.Switcher, ***performs a brute-force password guessing attack on the router's admin web interface****. If the attack succeeds, the malware changes the addresses of the DNS servers in the router's settings, thereby rerouting all DNS queries from devices in the attacked Wi-Fi network to the servers of the cybercriminals (such an attack is also known as DNS-hijacking)."*





```
admin:00000000
admin:admin
admin:123456
admin:12345678
admin:123456789
admin:1234567890
admin:66668888
admin:1111111
admin:88888888
admin:666666
admin:87654321
admin:147258369
admin:987654321
admin:66666666
admin:112233
admin:888888
admin:000000
admin:5201314
admin:789456123
admin:123123
admin:789456123
admin:0123456789
admin:123456789a
admin:11223344
admin:123123123
```

http://www.zdnet.com/article/this-android-infecting-trojan-malware-uses-your-phone-to-attack-your-router/

Nightmare #7

The security community will continue to point out flaws in IoT devices within the security echo chamber, and not affect change in the industries producing IoT devices.

I See Vulnerabilities

Was going to drop 85 vulnerabilities

Someone beat him to the punch

Good news, there are 83 left unpatched

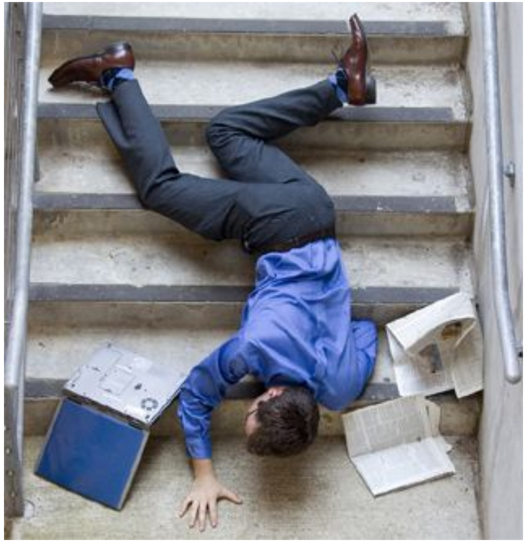
Also, he shredded several other devices

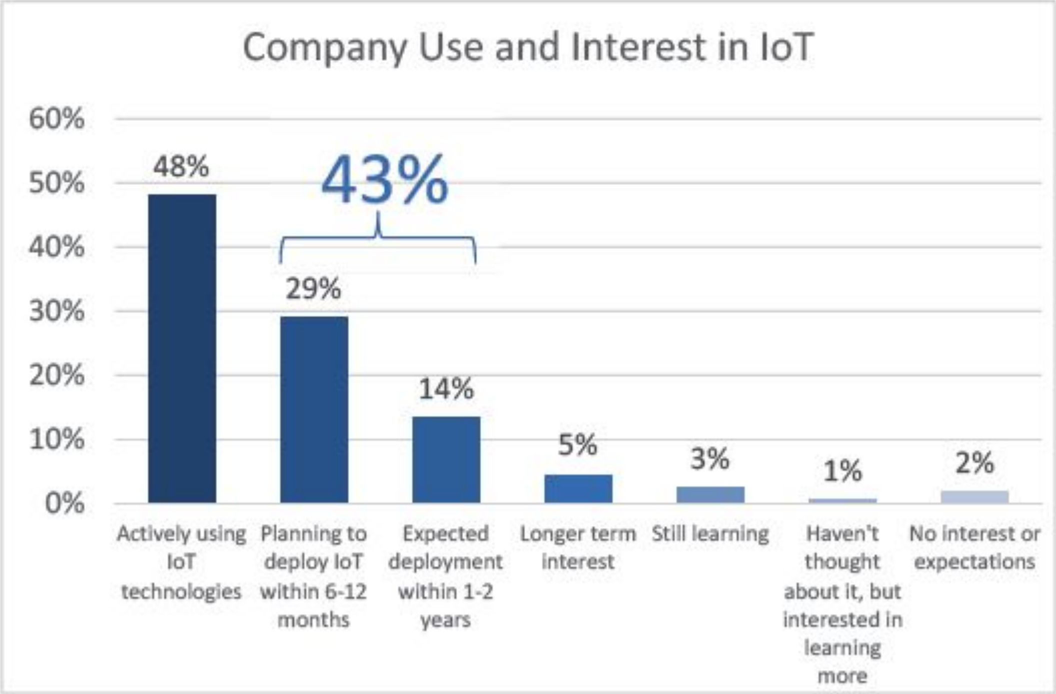
Then said he can find so many bugs that the disclosure process is terrible

https://threatpost.com/travel-routers-nas-devices-among-easily-hacked-iot-devices/124877/

Nightmare #8

Enterprises will adopt IoT technology (knowingly or not) and not incorporate security into the implementation

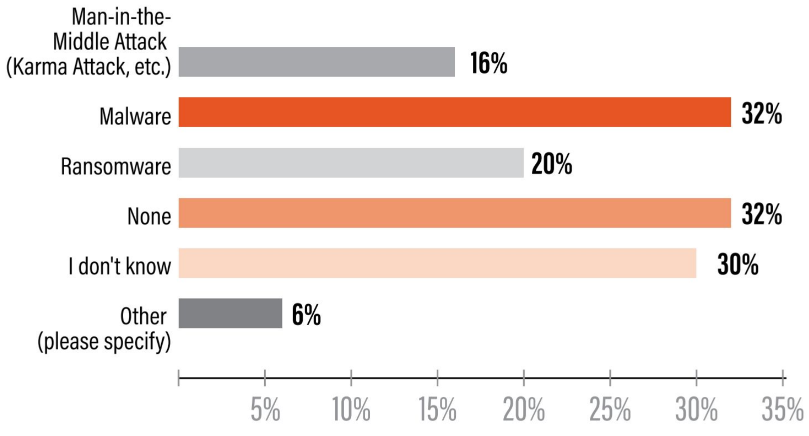




"Machina Research conducted a TIA-commissioned survey in March/April 2016 covering 200 business decision makers in US companies with annual revenues of at least $10 million (average annual revenue was $425m)."

http://www.zdnet.com/article/enterprise-iot-in-2017-the-state-of-play/

GRAPH 04 **WHAT TYPES OF ATTACKS HAVE HIT YOUR IOT DEVICES IN THE LAST YEAR? CHECK ALL THAT APPLY.**



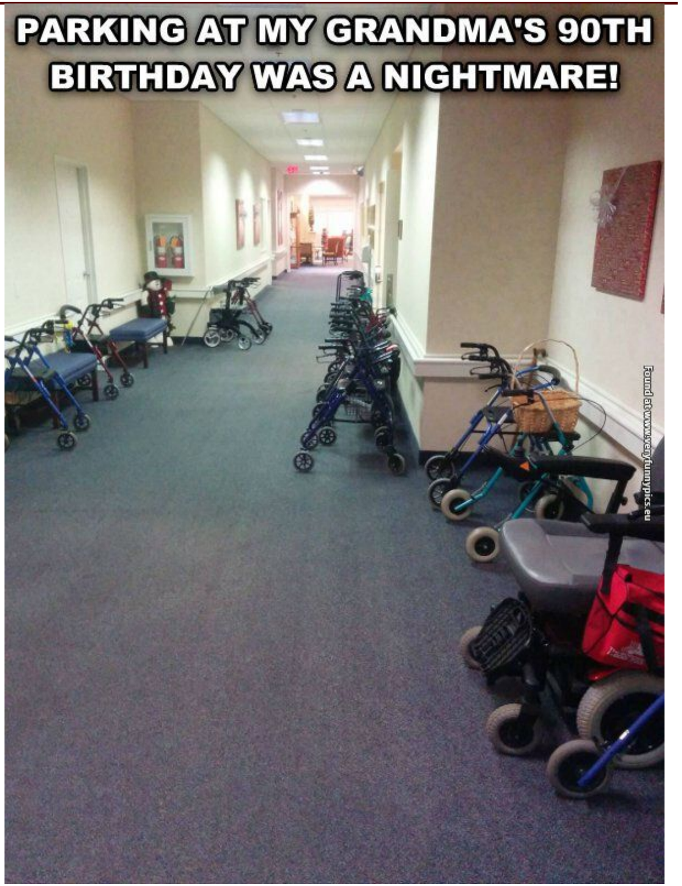
Number of respondents: 868

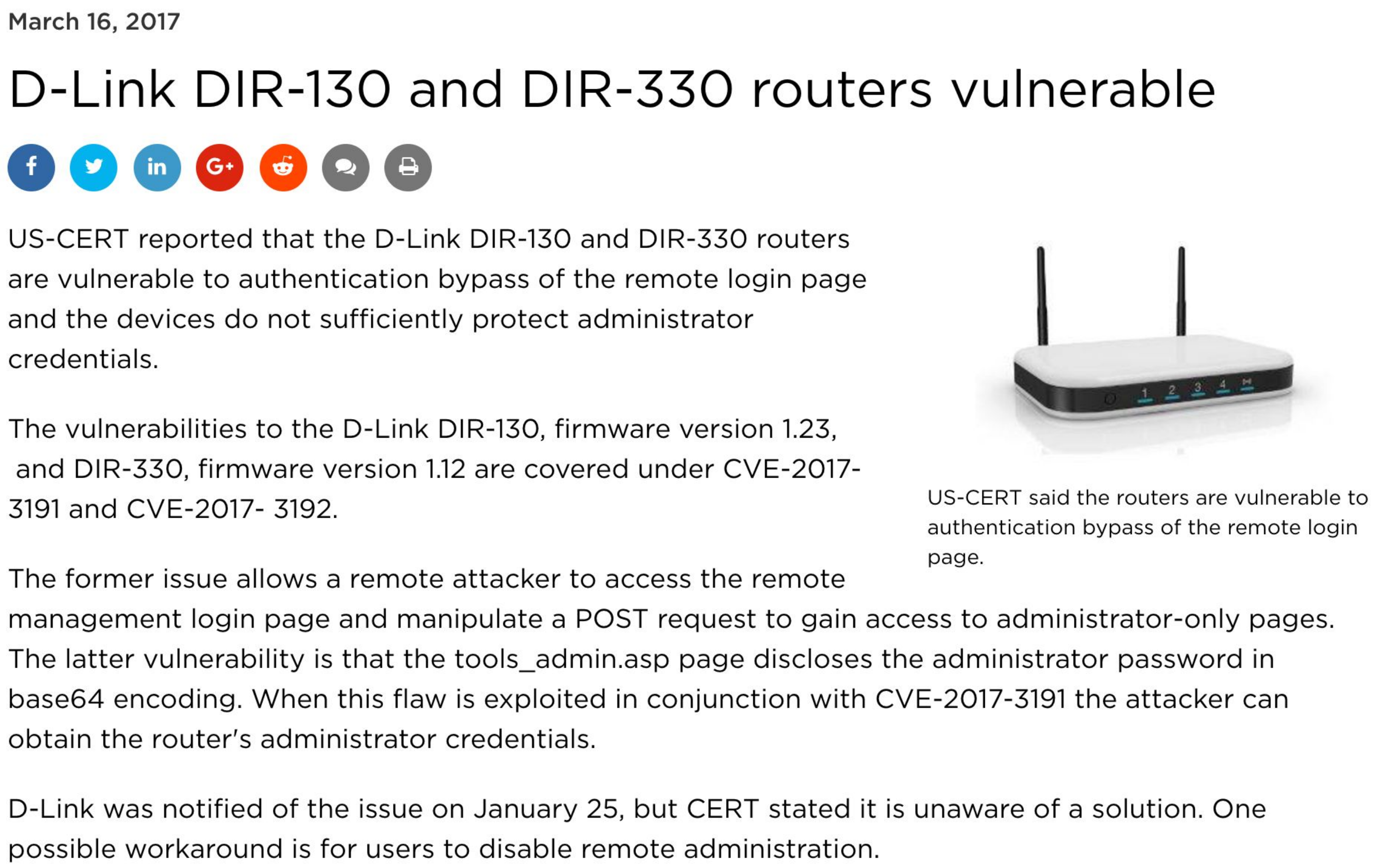
The report’s findings were culled from a survey of more than 800 IT security professionals and on-the-ground data from Pwnie Express sensors monitoring real life wired, wireless, IoT, and BYOD device data **gathered from a wide range of businesses across industries including financial services, hospitality, retail, manufacturing, professional services, technology, healthcare, energy** and more.

https://www.pwnieexpress.com/2017-internet-of-evil-things-report

Nightmare #9

D-Link, Linksys and others will still produce vulnerable products with the same exposures as the past and not improve security


PARKING AT MY GRANDMA'S 90TH BIRTHDAY WAS A NIGHTMARE!
Found at www.veryfunnypics.eu



March 16, 2017

D-Link DIR-130 and DIR-330 routers vulnerable

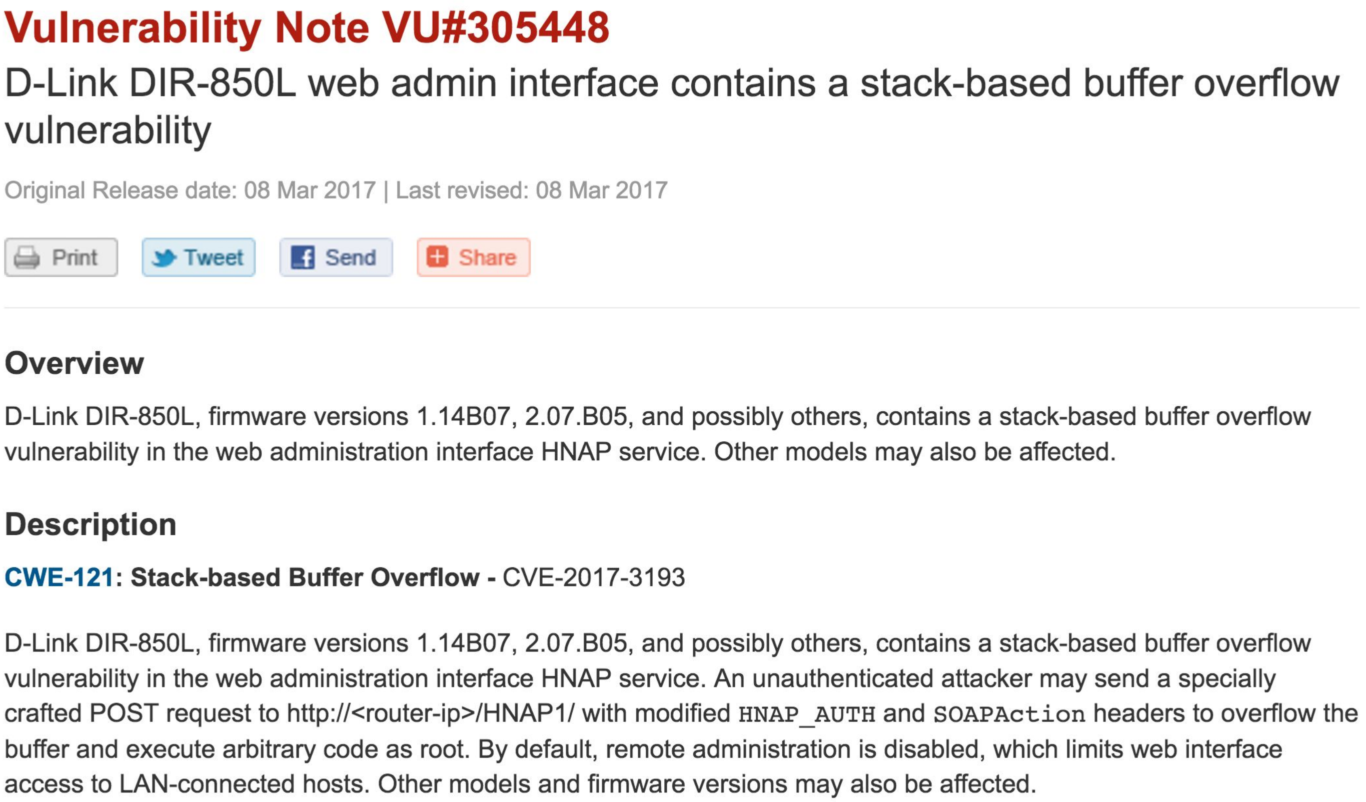
US-CERT reported that the D-Link DIR-130 and DIR-330 routers are vulnerable to authentication bypass of the remote login page and the devices do not sufficiently protect administrator credentials.

The vulnerabilities to the D-Link DIR-130, firmware version 1.23, and DIR-330, firmware version 1.12 are covered under CVE-2017-3191 and CVE-2017- 3192.

US-CERT said the routers are vulnerable to authentication bypass of the remote login page.

The former issue allows a remote attacker to access the remote management login page and manipulate a POST request to gain access to administrator-only pages. The latter vulnerability is that the tools_admin.asp page discloses the administrator password in base64 encoding. When this flaw is exploited in conjunction with CVE-2017-3191 the attacker can obtain the router's administrator credentials.

D-Link was notified of the issue on January 25, but CERT stated it is unaware of a solution. One possible workaround is for users to disable remote administration.



Vulnerability Note VU#305448

D-Link DIR-850L web admin interface contains a stack-based buffer overflow vulnerability

Original Release date: 08 Mar 2017 | Last revised: 08 Mar 2017

Overview

D-Link DIR-850L, firmware versions 1.14B07, 2.07.B05, and possibly others, contains a stack-based buffer overflow vulnerability in the web administration interface HNAP service. Other models may also be affected.

Description

CWE-121: Stack-based Buffer Overflow - CVE-2017-3193

D-Link DIR-850L, firmware versions 1.14B07, 2.07.B05, and possibly others, contains a stack-based buffer overflow vulnerability in the web administration interface HNAP service. An unauthenticated attacker may send a specially crafted POST request to http://<router-ip>/HNAP1/ with modified `HNAP_AUTH` and `SOAPAction` headers to overflow the buffer and execute arbitrary code as root. By default, remote administration is disabled, which limits web interface access to LAN-connected hosts. Other models and firmware versions may also be affected.

Protocols…

Defcon 22 (2014) Shahar SHREDS TR-069 security (or lack thereof)

TOP SECRET//SI//REL TO DC22

22 DEFCON

(U) I hunt TR-069 admins

PWNING ISPS LIKE A BOSS

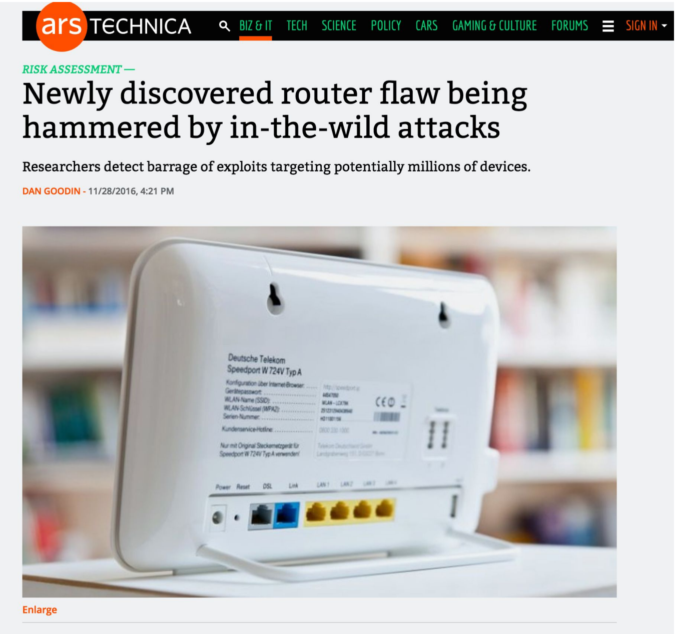
Shahar Tal

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

https://www.defcon.org/images/defcon-22/dc-22-presentations/Tal/DEFCON-22-Shahar-Tal-I-hunt-TR-069-admins-UPDATED.pdf

Vendor/ISP Response

November 2016 - TR-069 CHAOS



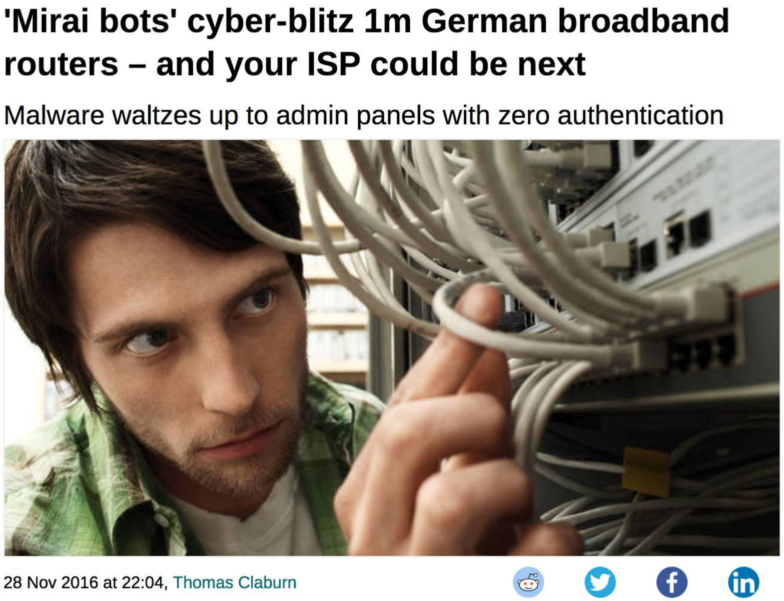
RISK ASSESSMENT —

Newly discovered router flaw being hammered by in-the-wild attacks

Researchers detect barrage of exploits targeting potentially millions of devices.

DAN GOODIN - 11/28/2016, 4:21 PM

Enlarge



'Mirai bots' cyber-blitz 1m German broadband routers – and your ISP could be next

Malware waltzes up to admin panels with zero authentication

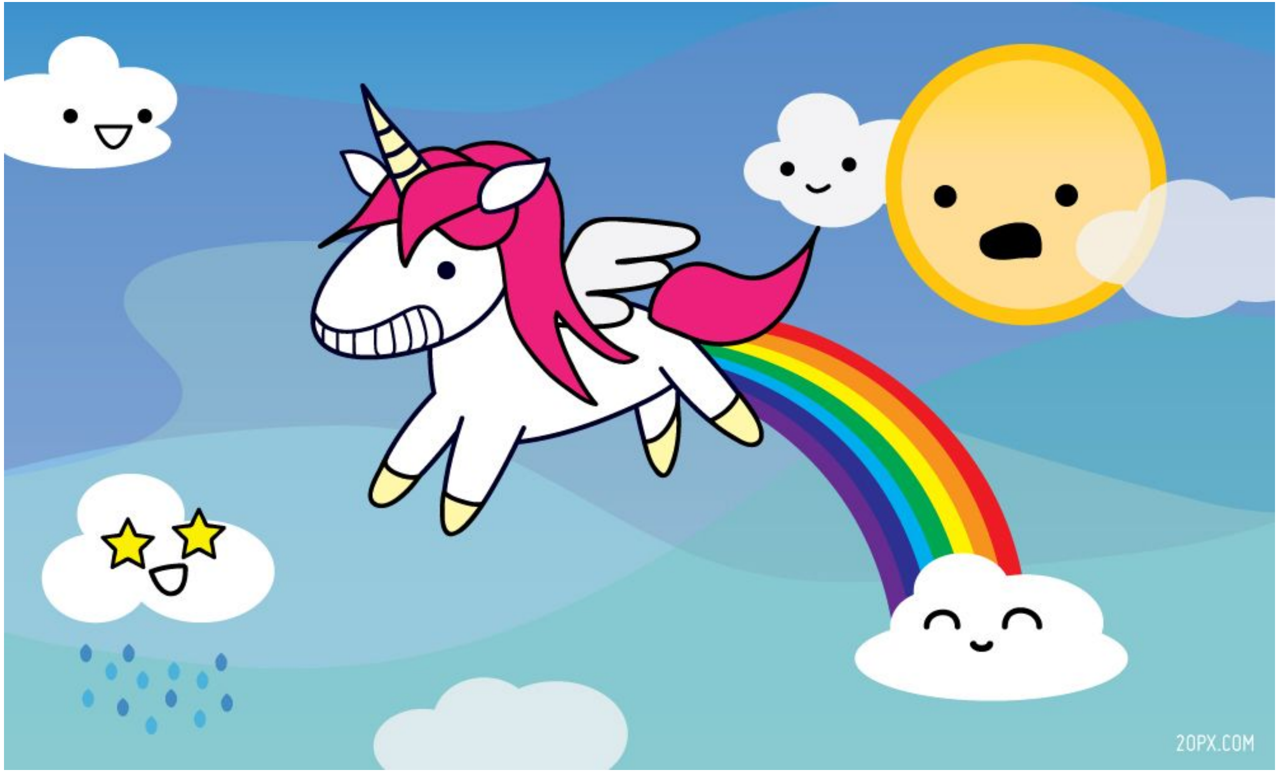
28 Nov 2016 at 22:04, Thomas Claburn

https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/

Nightmare #10

The industry would coin a horrible acronym for embedded devices, the average person has more than one of said devices, none of the security problems would be addressed and I would be forced once again to present on the topic…

Crap...

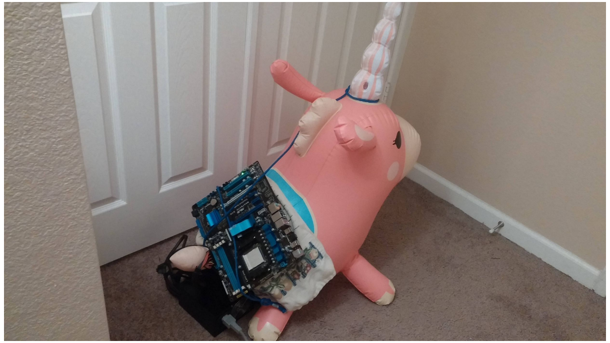


Glimmers of Hope…

“Regulation will be far worse without the involvement of the community and guidance from those in the know”

The FTC & Asus

Asus was bad, allowed everyone to manage your storage!

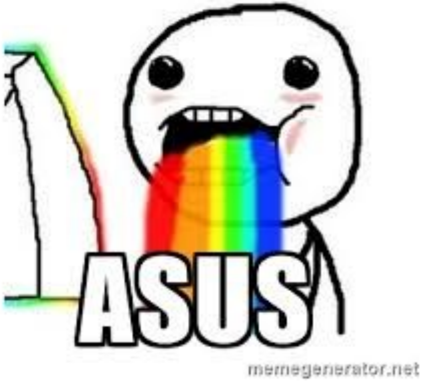


This greatly displeased the FTC, so they filed suit against Asus

The FTC specifically called out default passwords!

Asus now has to comply with 20 years of audits, of which I can find no details

https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put



The FTC & D-Link

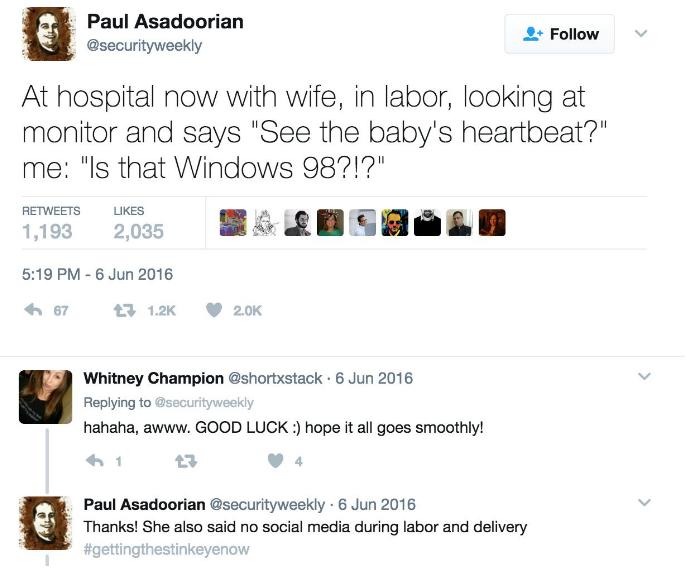
https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate

*“D-Link promoted the security of its routers on the company’s website, which included materials headlined “**EASY TO SECURE**” and “**ADVANCED NETWORK SECURITY.**”*

“D-Link Systems, Inc. will vigorously defend itself against the unwarranted and baseless charges made by the Federal Trade Commission (FTC). "

https://www.engadget.com/2017/01/13/ftc-vs-d-link-all-bark-no-bite/

The FDA



Paul Asadoorian
@securityweekly

Follow

At hospital now with wife, in labor, looking at monitor and says "See the baby's heartbeat?" me: "Is that Windows 98?!?"

RETWEETS	LIKES
1,193	2,035

5:19 PM - 6 Jun 2016

↩ 67 1.2K ♥ 2.0K

Whitney Champion @shortxstack · 6 Jun 2016
Replying to @securityweekly
hahaha, awww. GOOD LUCK :) hope it all goes smoothly!

↩ 1 ♥ 4

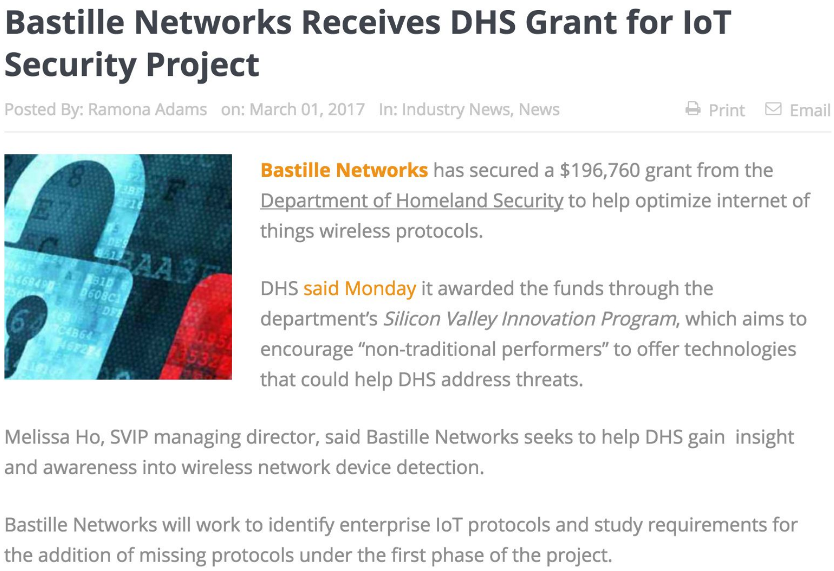
Paul Asadoorian @securityweekly · 6 Jun 2016
Thanks! She also said no social media during labor and delivery
#gettingthestinkeyenow

Josh Corman and Katie Mousris joined us to discuss the state of security for the healthcare community (episode 479)

http://www.eweek.com/security/medical-device-security-guidance-released-by-fda-as-threats-multiply.html

https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

NIST, DHS & NSF



Bastille Networks Receives DHS Grant for IoT Security Project

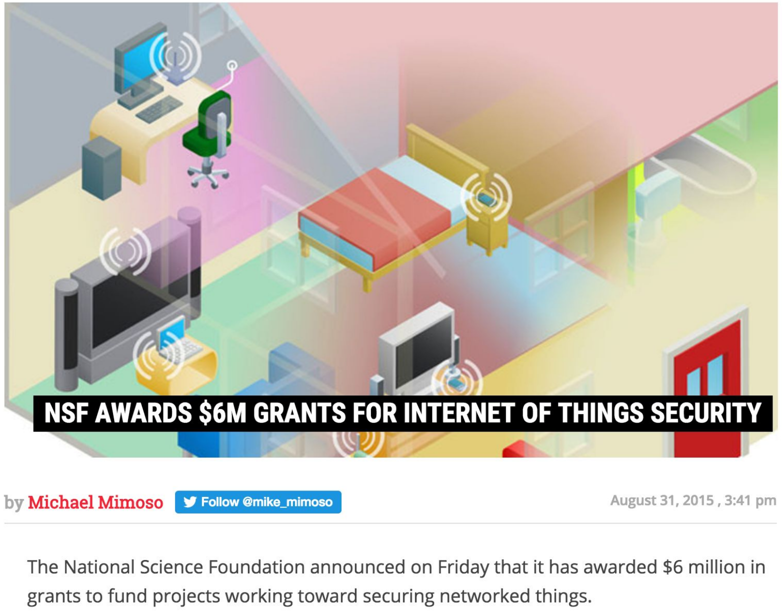
Posted By: Ramona Adams on: March 01, 2017 In: Industry News, News Print Email

Bastille Networks has secured a $196,760 grant from the Department of Homeland Security to help optimize internet of things wireless protocols.

DHS said Monday it awarded the funds through the department's *Silicon Valley Innovation Program*, which aims to encourage "non-traditional performers" to offer technologies that could help DHS address threats.

Melissa Ho, SVIP managing director, said Bastille Networks seeks to help DHS gain insight and awareness into wireless network device detection.

Bastille Networks will work to identify enterprise IoT protocols and study requirements for the addition of missing protocols under the first phase of the project.



NSF AWARDS $6M GRANTS FOR INTERNET OF THINGS SECURITY

by Michael Mimoso Follow @mike_mimoso August 31, 2015 , 3:41 pm

The National Science Foundation announced on Friday that it has awarded $6 million in grants to fund projects working toward securing networked things.

https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

CyberUL

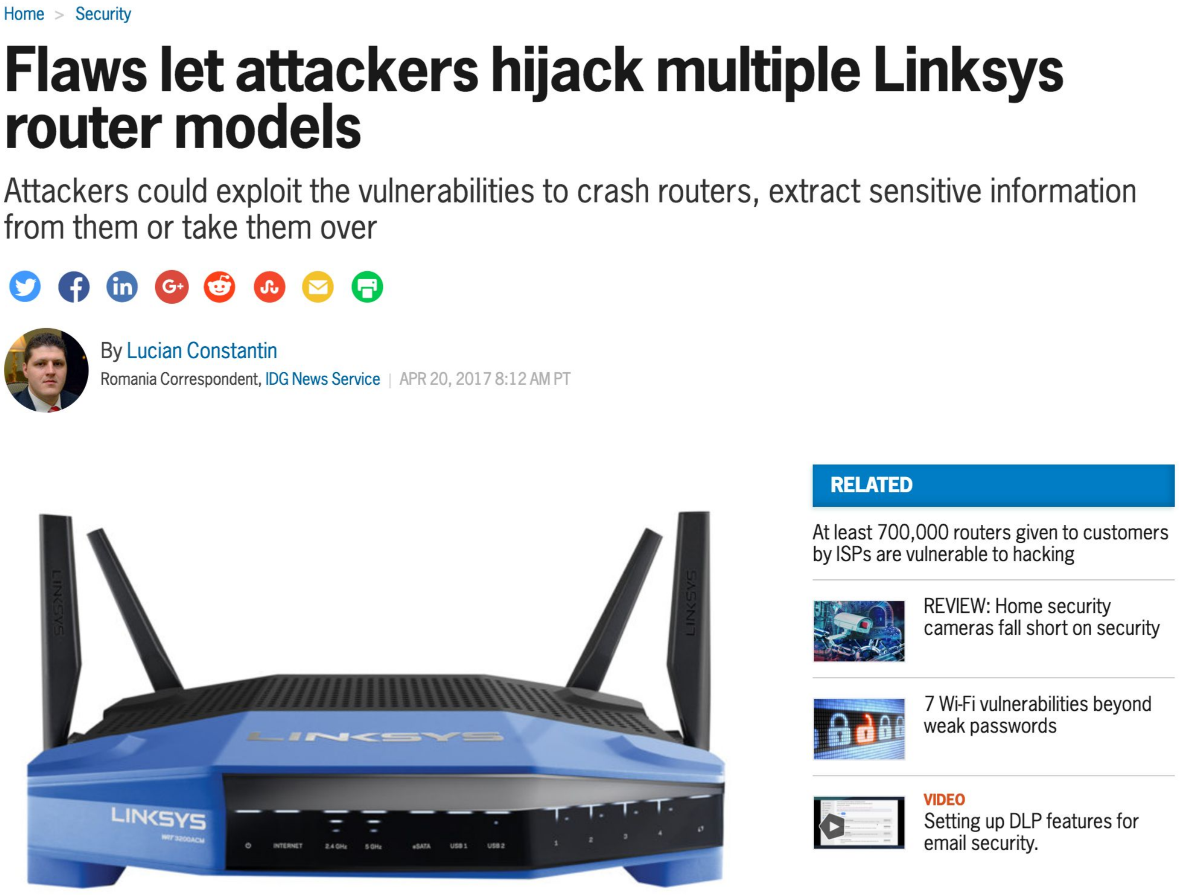
Mudge is leading the effort to create standards (for testing and implementation) of IoT devices

Of course, different people are in the White House today, who are not necessarily in support of Government standards

Some disagree, but I believe this is a good idea that needs our support and experience (continue free market capitalism, but provide safe standards, tricky!)

- http://blog.erratasec.com/2015/06/cyberul-is-dumb-idea.html#.WH-BibYrLFw
- http://www.darkreading.com/vulnerabilities---threats/cyberul-launched-for-iot-critical-infrastructure-device-security-/d/d-id/1324985
- https://threatpost.com/cyber-ul-could-become-reality-under-leadership-of-hacker-mudge/113538/

Disclosure Is Getting Better



Home > Security

Flaws let attackers hijack multiple Linksys router models

Attackers could exploit the vulnerabilities to crash routers, extract sensitive information from them or take them over

By Lucian Constantin
Romania Correspondent, IDG News Service | APR 20, 2017 8:12 AM PT

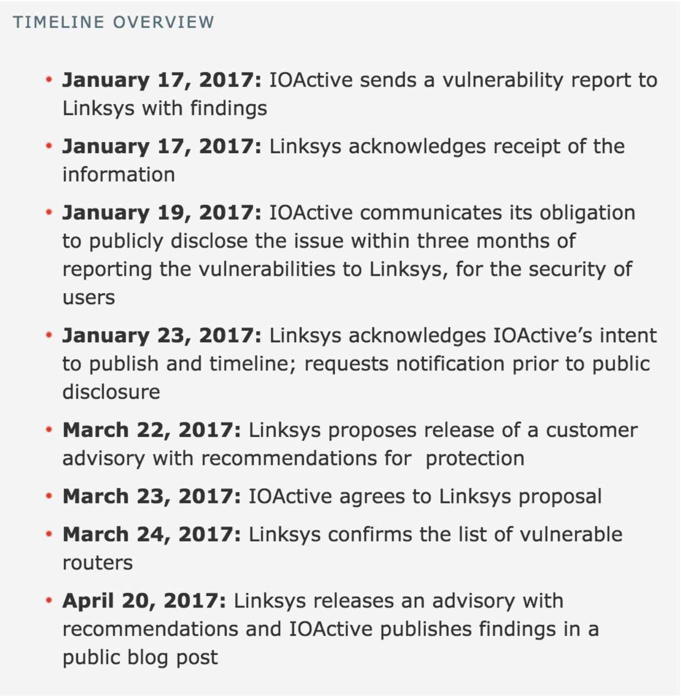
RELATED

At least 700,000 routers given to customers by ISPs are vulnerable to hacking

REVIEW: Home security cameras fall short on security

7 Wi-Fi vulnerabilities beyond weak passwords

VIDEO
Setting up DLP features for email security.

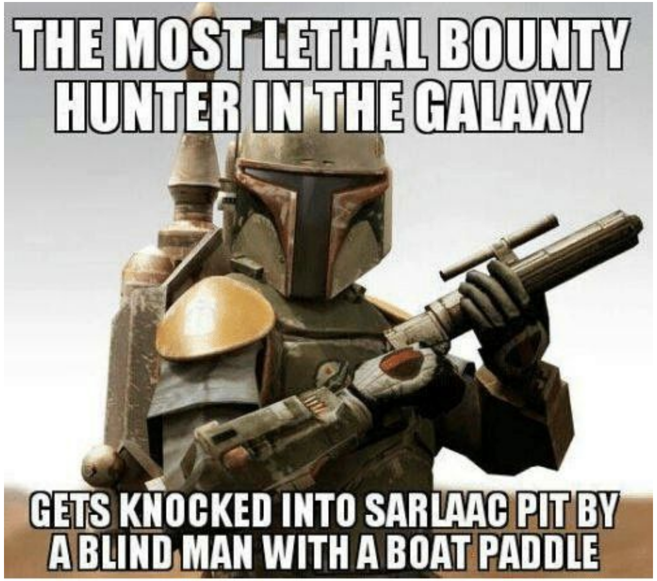


TIMELINE OVERVIEW

- **January 17, 2017:** IOActive sends a vulnerability report to Linksys with findings
- **January 17, 2017:** Linksys acknowledges receipt of the information
- **January 19, 2017:** IOActive communicates its obligation to publicly disclose the issue within three months of reporting the vulnerabilities to Linksys, for the security of users
- **January 23, 2017:** Linksys acknowledges IOActive’s intent to publish and timeline; requests notification prior to public disclosure
- **March 22, 2017:** Linksys proposes release of a customer advisory with recommendations for protection
- **March 23, 2017:** IOActive agrees to Linksys proposal
- **March 24, 2017:** Linksys confirms the list of vulnerable routers
- **April 20, 2017:** Linksys releases an advisory with recommendations and IOActive publishes findings in a public blog post

Bug Bounties

- https://bugcrowd.com/netgear
- https://hackerone.com/linksys
- https://samsungtvbounty.com/
- https://hackerone.com/ubnt
- https://bugcrowd.com/customers/wink


THE MOST LETHAL BOUNTY HUNTER IN THE GALAXY
GETS KNOCKED INTO SARLAAC PIT BY A BLIND MAN WITH A BOAT PADDLE

Paul Asadoorian

paul@securityweekly.com

@securityweekly