nic.br cgi.br cert.br

**II Encontro Anual da
Academia Nacional de Engenharia**

Rio de Janeiro, RJ
25 de novembro de 2016

Segurança na Sociedade Digital: Novos Desafios, Velhos Problemas

Cristine Hoepers, D.Sc.
cristine@cert.br

Cristine Hoepers, D.Sc.
cristine@cert.br

cert.br   nic.br   cgi.br

A sociedade está permeada de objetos conectados
Estamos cientes dos riscos?

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts

Technology

Osram Lightify light bulbs 'vulnerable to hack'

🕐 27 July 2016 | T

Security researchers have discovered nine vulnerabilities in a range of internet-connected light bulbs made by Osram.

The flaws in the Lightify products <u>could give attackers access to a home wi-fi network</u>, and potentially operate the lights without permission.

Osram said a "majority" of the problems would be fixed in a software update in August, but four remained unpatched.

One security expert said Osram had made an "elementary" mistake.

http://www.bbc.com/news/technology-36903274

cert.br nic.br cgi.br

Why Light Bulbs May Be the Next Hacker Target

By JOHN MARKOFF   NOV. 3, 2016

Researchers report in a paper to be made public on Thursday that they have uncovered a flaw in a wireless technology that is often included in smart home devices like lights, switches, locks, thermostats and many of the components of the much-ballyhooed "smart home" of the future.

The researchers focused on the Philips Hue smart light bulb and found that the wireless flaw could allow hackers to take control of the light bulbs, according to researchers at the Weizmann Institute of Science near Tel Aviv and Dalhousie University in Halifax, Canada.

And they wouldn't have to have direct access to the devices to infect them: The researchers were able to spread infection in a network inside a building by driving a car 229 feet away.

The new risk comes from a little-known radio protocol called ZigBee. Created in the 1990s, ZigBee is a wireless standard widely used in home consumer devices. While it is supposed to be secure, it hasn't been held up to the scrutiny of other security methods used around the internet.

The Internet of Things, a
it may also prove irresist

http://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r=1

cert.br nic.br cgi.br

Bitdefender® LABS

Hackers Can Use Smart Sockets to Shut Down Critical Systems

Users might be risking their privacy, and even physical security, when using smart plugs to manage appliances in

Password remote control

If an attacker knows the MAC address of the device and the default password, he can gain remote control of the device to re-schedule it, or access all the information the device uses, including the user's email address and password, if the email notification feature is enabled. This can lead to the full compromise of the linked email account, unless two-factor authentication is enabled.

Firmware upgrade through command injection

The device hashes its own credentials using the MD5 algorithm. Hashing means that, for every input (string of data), a hash delivers a unique value of 32 characters. This is done through the md5sum command, which receives the joined username and password as a parameter.

https://labs.bitdefender.com/2016/08/hackers-can-use-smart-sockets-to-shut-down-critical-systems/

Vulnerability Note VU#719736

Fisher-Price Smart Toy platform allows some unauthenticated web API commands

Original Release date: 02 Feb 2016 | Last revised: 02 Feb 2016

🖶 Pr

Impact

A remote attacker may be able to view or edit private information about the child and/or parent that registers the toy, and may take over ownership of the toy.

Overview

The Fisher-Price Smart Toy does not perform proper authentication of some API commands, and it may also use a vulnerable version of Android.

Description

The Fisher-Price Smart Toy bear is a new WiFi-connected Internet of Things (IoT) toy. The device utilizes network connectivity to provide more interactivity with children.

CWE-287: Improper Authentication - CVE-2015-8269

The Fisher-Price Smart Toy uses a predictable account number which may allow an attacker that has signed up for the Fisher-Price Smart Toy platform to perform some queries and commands on other accounts. Such queries may allow an attacker to learn name, birthday, gender, and other details of the user. An attacker may also edit some personal details, and re-associate the toy to a different account.

According to the researchers at Rapid7, not all data is modifiable or reachable, somewhat mitigating the impact: Furthermore, the researcher notes the Smart Toy is based on Android 4.4 (KitKat). It is currently not clear if the platform is updated with the latest Android security patches.

http://www.kb.cert.org/vuls/id/719736

cert.br nic.br cgi.br

SMART OPTIONS FOR RELIABLE MEDICATION DELIVERY

Hospira high-performance infusion pumps make it easy for you to deliver exceptional patient safety and care. Our focused portfolio features proven, innovative smart pump and pain management technology designed to help meet your clinical safety and workflow goals. The powerful Hospira MedNet™ safety software helps to reduce medication errors and raise the bar for your medication management system. And, with an eye to the future, our Plum™ family of smart pumps with Hospira MedNet are designed to integrate with your electronic medical record (EMR) systems through our IV Clinical Integration solution.

Our focused line of infusion systems includes general infusion and pain management pumps:

PLUM 360™ INFUSION SYSTEM
Your direct connection to clinical excellence with integrated safety and efficiency at every step.

Advisory (ICSA-15-161-01)

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

Original release date: June 10, 2015 | Last revised: June 12, 2015

STACK-BASED BUFFER OVERFLOW[b]

The researcher has evaluated the device and asserts that the device contains a buffer overflow vulnerability that could be exploited to allow execution of arbitrary code on the device. This vulnerability has not been validated by Hospira. However, acting out of an abundance of caution, ICS-CERT is including this information to enhance healthcare providers' awareness, so that additional monitoring and controls can be applied.

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[d]

IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP. Hospira has not validated claims of firmware updates and pump commands for Plum A+ and Plum A+3 from unauthorized devices on the host network.

cert.br nic.br cgi.br

Vulnerability Note VU#884840

Animas OneTouch Ping insulin pump contains multiple vulnerabilities

Original Release date: 04 Oct 2016 | Last revised: 11 Oct 2016

Print   Tweet   Send   Share

Overview

The Animas OneTouch Ping insulin pump contains multiple vulnerabilities that may allow an unauthenticated remote attacker to obtain patient treatment or device data, or execute commands on the device. The attacker cannot obtain personally identifiable information.

Johnson and Johnson has provided the following statement:

"There are no plans to release a firmware update, however a notification is being sent to patients and HealthCare Professionals. In addition, there are a number of documented and proprietary mitigating controls in place to ensure the safe delivery of insulin, outlined below.

i. If patients are concerned about unauthorized access for any reason, the pump's radio frequency feature can be turned off, which is explained in Chapter 2 of Section III of the OneTouch® Ping® Owner's Booklet. However, turning off this feature means that the pump and meter will no longer communicate and blood glucose readings will need to be entered manually on the pump.

ii. If patients choose to use the meter remote feature, another option for protection is to program the OneTouch® Ping® pump to limit the amount of bolus insulin that can be delivered. Bolus deliveries can be limited through a

iii. The company also suggests turning on the Vibrating Alert feature of the OneTouch® Ping® System, as described in Chapter 4 of Section I. This notifies the user that a bolus dose is being initiated by the meter remote, which gives the patient the option of canceling the bolus.

http://www.kb.cert.org/vuls/id/884840

cert.br   nic.br   cgi.br

Thousands of medical devices are vulnerable to hacking, security researchers

The security flaws put patients' health

James Niccolai   Sep 29, 2015 5:50 PM
IDG News Service

The same default passwords were used over and over for different models of a device, and in some cases a manufacturer warned customers that if they changed default passwords they might not be eligible for support. That's

Next time you go for an MRI scan, remember that the doctor might not be the only one who sees your results.

Thousands
infusion pu
security res

cert.br nic.br cgi.br

DDoS attack halts heating in Finland amidst winter

A Distributed Denial of Service (DDoS) attack halted heating distribution at least in two properties in the city of Lappeenranta, located in eastern Finland. In both of the events the attacks disabled the computers that were controlling heating in the buildings.

Both of the buildings where managed by Valtia. The company who is in charge of managing the buildings overall and maintenance. According to CEO, Simo Rounela, in both cas circulation were temporarily disa

Building Automation security is not a priority

The devices under attack were built by the company Fidelix. According to company representative Antti Koskinen, there have been other attacks in the country before the case in Lappeenranta. He also states to Helsingin Sanomat that when people want convenience and ease of use it often opens up vulnerabilities.

cert.br nic.br cgi.br

CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

CWE-798: Use of Hard-coded Credentials - CVE-2013-3612

All DVRs of the same series ship with the same default root password on a read-only partition. Therefore, the root password can only be changed by flashing the firmware. Additionally, a separate hard-coded remote backdoor account exists that can be used to control cameras and other system components remotely. It is only accessible if authorization is done through ActiveX or the stand-alone client. Additionally, a hash of the current date can be used as a master password to gain access to the system and reset the administrator's password.

Vulnerability Note VU#800094

Dahua Security DVRs contain multiple vulnerabilities

Original Release date: 13 Sep 2013 | Last revised: 04 Dec 2013

🖨 Print   ➤ Tweet   f Send   ⊕ Share

Overview

Digital video recorders (DVR) produced by Dahua Technology Co., Ltd. contain multiple vulnerabilities that could allow a remote attacker to gain privileged access to the devices.

Botnets de Dispositivos IoT

Botnets: redes de dispositivos infectados, controladas por atacantes

Evolução sendo acompanhada em nossa rede de sensores desdes 2013

– infectam CPEs, DVRs, CCTVs, NAS, roteadores domésticos, etc

Malware **se propaga geralmente via Telnet**

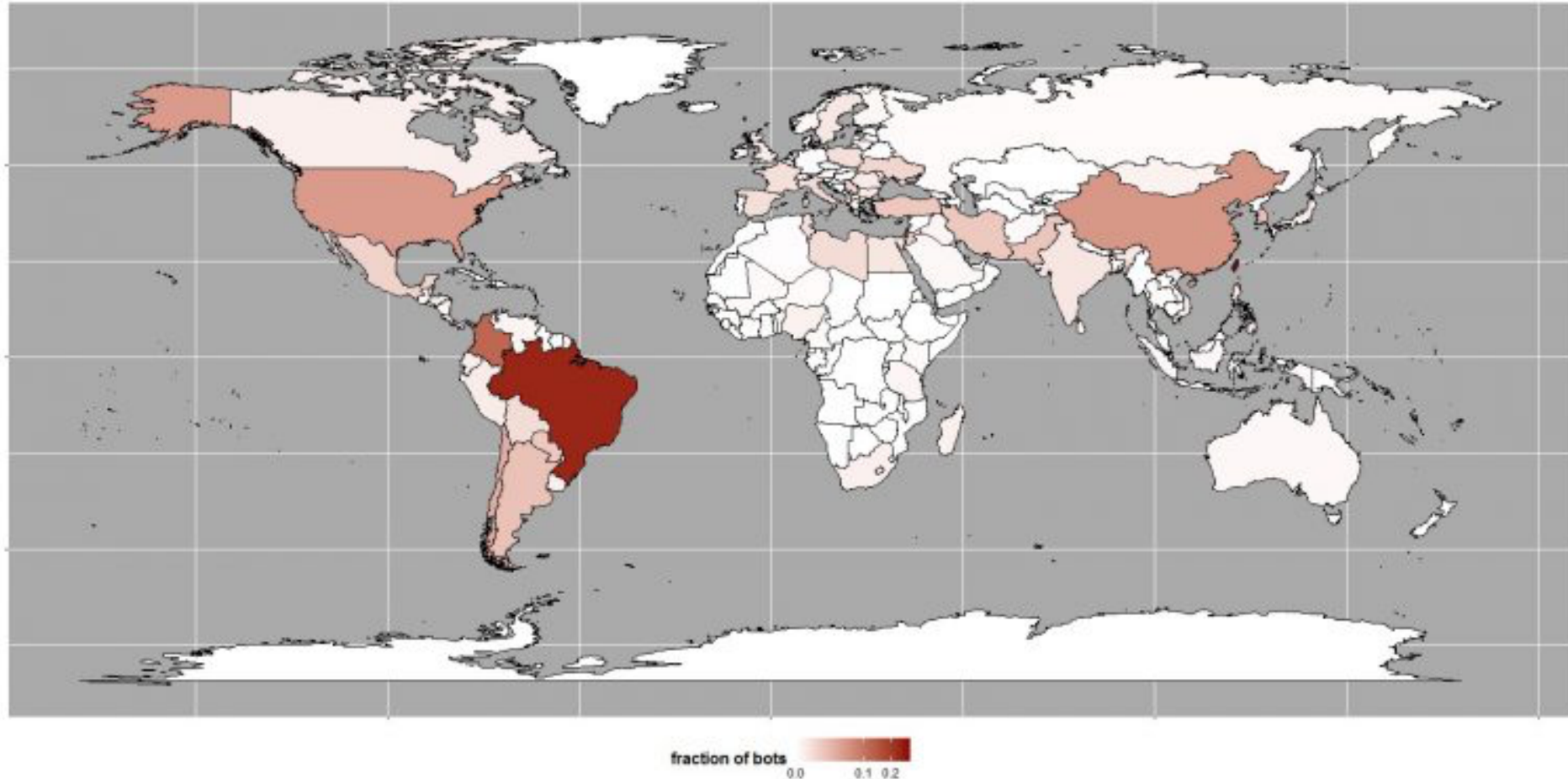– protocolo para conexão remota, sem criptografia

Explora Senhas Fracas ou Padrão

– muitas vezes são "*backdoors*" dos fabricantes

Foco em dispositivos com versões "enxutas" de Linux

– para sistemas embarcados

– arquiteturas ARM, MIPS, PowerPC, etc

Variante mais antiga sendo monitorada:
gafgyt (ou também Lizkebab, BASHLITE, Torlus)

fraction of bots
0.0 0.1 0.2

Fonte: Estatísticas da distribuição global, Level3, 25 de agosto de 2016

cert.br nic.br cgi.br

Setembro/2016, variante Mirai é identificada:
620Gbps contra o Blog do Brian Krebs

– Maior ataque de negação de serviço (DDoS) registrado até então

BBC NEWS

Massive web attack hits security blogger

22 September 2016 | Technology

The distributed denial of service (DDoS) attack was aimed at the **website** of industry expert Brian Krebs.

At its peak, the attack aimed 620 gigabits of data a second at the site.

Text found in attack data packets suggested it was mounted to protest against Mr Krebs' work to uncover who was behind a prolific DDoS attack.

http://www.bbc.co.uk/news/amp/37439513

cert.br nic.br cgi.br

Roteadores 4G–WiFi Sierra Wireless

- utilizados, entre outros, em: gasodutos, oleodutos, semáforos, iluminação pública, smart grids, carros de polícia e ambulâncias

SIERRA WIRELESS

Sierra Wireless Technical Bulletin: Mirai Malware

Products: Sierra Wireless LS300, GX400, GX/ES440, GX/ES450 and RV50

Date of issue: 4 October 2016

Sierra Wireless has confirmed reports of the "Mirai" malware infecting AirLink gateways that are using the default ACEmanager password and are reachable from the public internet. The malware is able to gain access to the gateway by logging into ACEmanager with the default password and using the firmware update function to download and run a copy of itself.

http://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin---mirai/

cert**.br** nic**.br** cgi**.br**

Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline

The sound of silence.

Brad Chacos | @BradChacos   Oct 21, 2016 3:34 PM
Senior Editor, PCWorld

http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html

cert.br nic.br cgi.br

Dados atualizados dos sensores do CERT.br:
Endereços IP únicos infectados com Mirai, por dia

IPs Infectados com Mirai: Total Mundial e Brasil

Período: 15/09/2016 a 23/11/2016
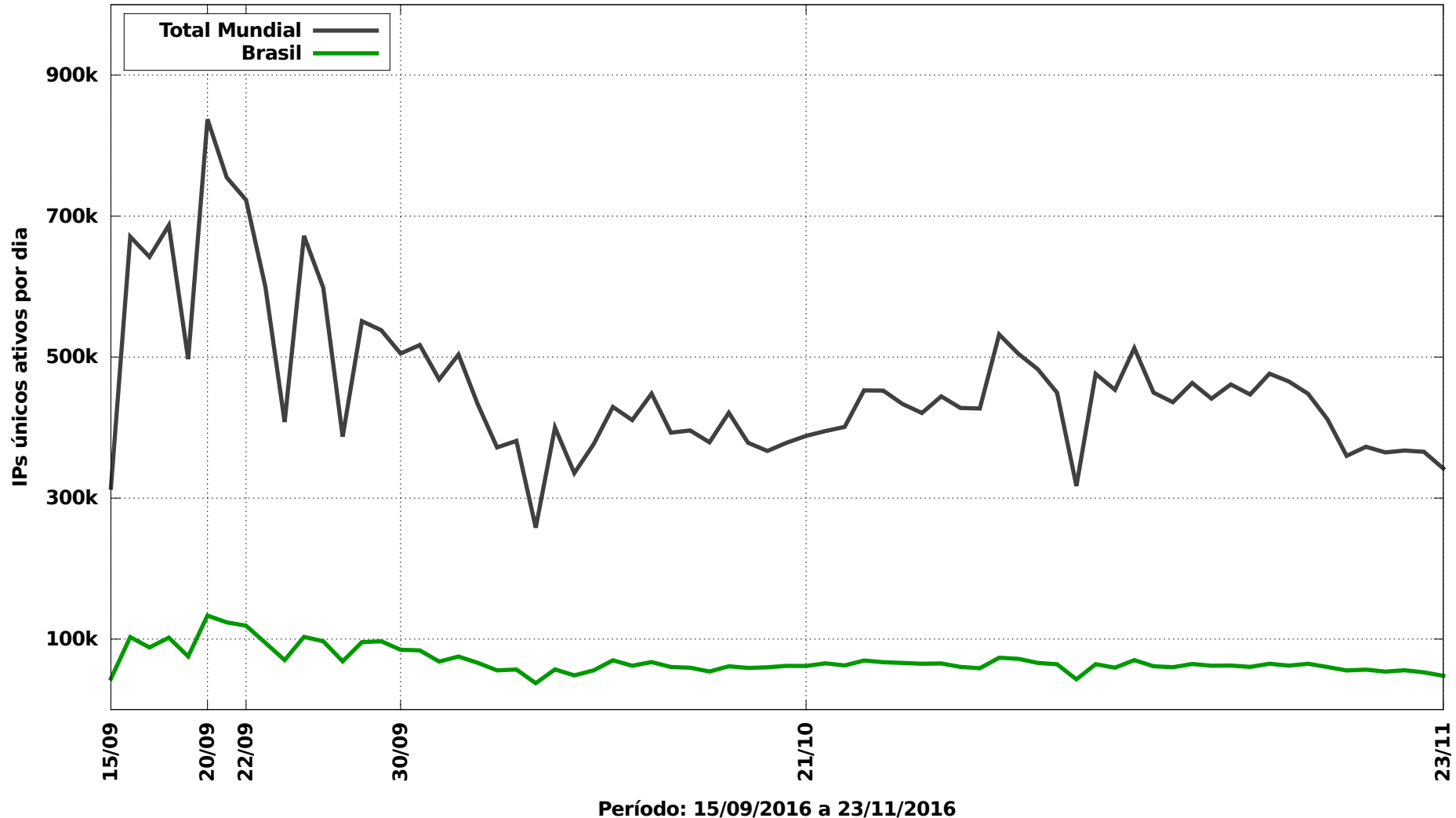
Em Comum, Velhos Problemas

Preocupação zero com cibersegurança

– "alguém" fará a segurança depois...

Falta de Autenticação

– para conectar

– para instalar componentes e enviar comandos

Autenticação fraca e "*backdoors*" do fabricante

– senhas padrão de fábrica

– senha do dia

– senha "para manutenção"

Agravante: empresas de diversos setores agora desenvolvem *software*, mas não agem como tal

– equipe de segurança de produto?

– planejamento de atualizações no ciclo de vida do produto?

– segurança de engenharia de *software*?

Como melhorar o cenário

Solução depende de diversas camadas

– usuários e administradores de sistemas

– desenvolvedores e fabricantes

Desenvolvedores / Fabricantes (1/2)

Segurança deve ser incluída na análise de risco

- danos à imagem
- danos aos usuários e à Internet como um todo

Segurança deve ser nativa

- não deve ser opcional
- requisitos de segurança devem ser considerados desde o projeto

Usar práticas de desenvolvimento seguro

Não usar protocolos obsoletos

Usar criptografia e autenticação forte

Não ter senha do dia, senha padrão não documentada, *reset* de configuração via rede, etc

***Defaults* seguros**

Desenvolvedores / Fabricantes (2/2)

Atualização precisa fazer parte do ciclo de vida

– precisa ser possível

– necessário prever algum mecanismo de autenticação

Necessário ter grupo de resposta a incidentes com produtos (PSIRT) preparado para lidar com os problemas

Planejar atualizações de segurança em larga escala

Desafio adicional em IoT: Um *chipset* ➔ diversos "fabricantes"

– Ex.: Dentre os fabricantes nacionais de câmeras, temos encontrando somente *chipsets* Dahua e Xiongmai

– Como atualizar? *Recall* consegue ser efetivo? (vide caso Xiongmai)

Usuários e Administradores de Sistemas (1/2)

Ser criterioso ao escolher o fornecedor
- – verificar se possui política de atualização de *firmware*
- – verificar histórico de tratamento de vulnerabilidades
- – identificar qual o *chipset*
  - – verificar histórico de tratamento de vulnerabilidades do fabricante do *chipset*
- – fazer testes antes de comprar
- – checar se é possível desabilitar serviços desnecessários e trocar senhas

Antes de fazer a implantação, planejar
- – se haverá algum esquema de gerência remota
- – como atualizar remotamente

Mesmo escolhendo criteriosamente o fornecedor, assumir que os dispositivos virão com sérios problemas

- testar em ambiente controlado
- assumir que terá um "*backdoor*" do fabricante

Desabilitar serviços desnecessários e mudar senhas padrão

- nem sempre é possível, vide DVRs e Câmeras

Manter os equipamentos atualizados

Utilizar sempre que possível uma rede de gerência

- isolar os dispositivos completamente

Obrigada

www.cert.br

@ cristine@cert.br   🅣 @certbr

25 de novembro de 2016

nic.br   cgi.br

www.nic.br | www.cgi.br