

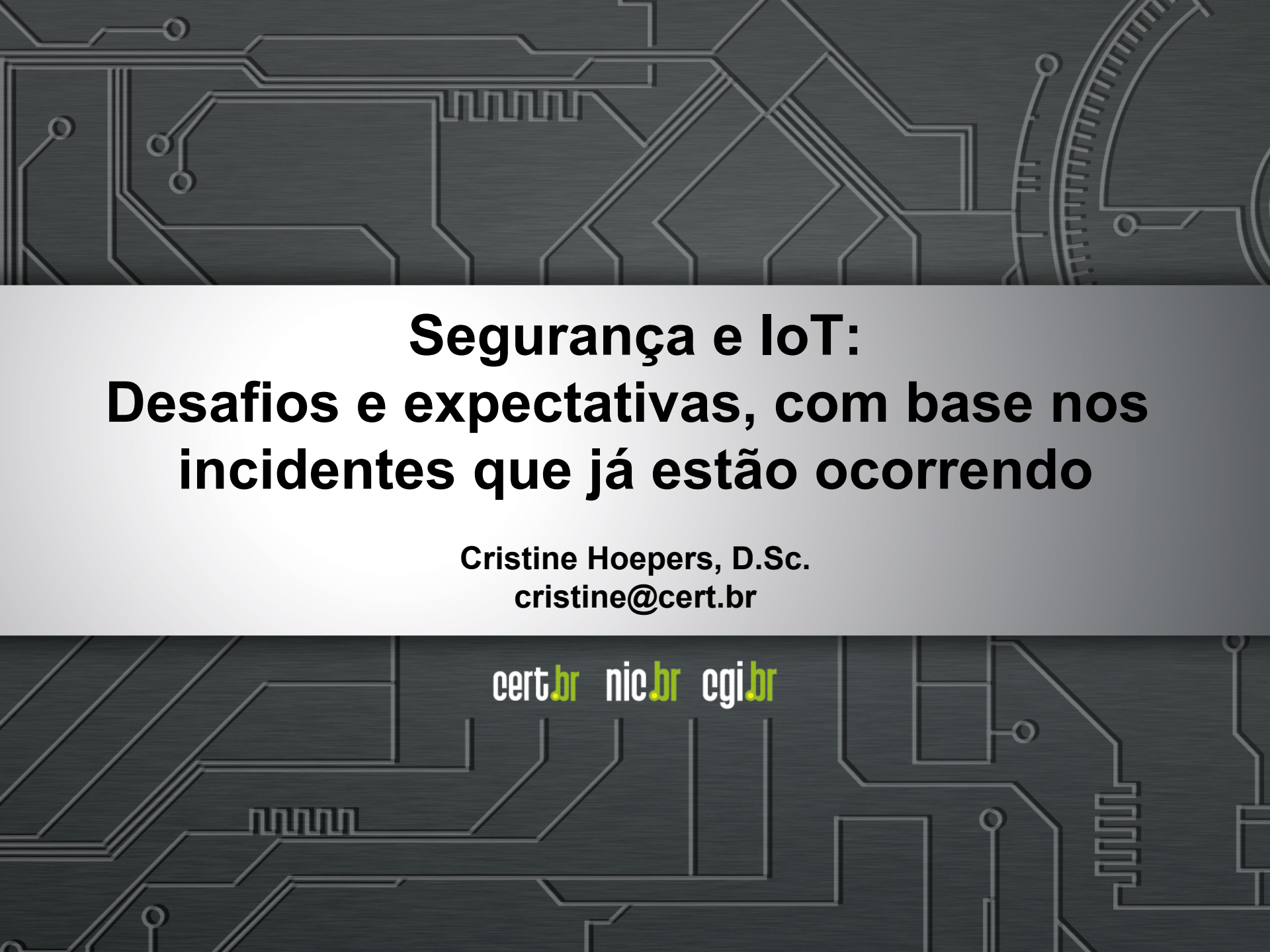
nic.br egi.br

cert.br

3º Cyber Security Brazil – Energy & Utilities

São Paulo, SP

28 de março de 2017



Segurança e IoT: Desafios e expectativas, com base nos incidentes que já estão ocorrendo

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

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:

Contact Hospira



PLUM 360™ INFUSION SYSTEM

Your direct connection to clinical excellence with integrated safety and efficiency at every step.

Advisory (ICSA-15-161-01)

[More Advisories](#)

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 unauthenticated devices on the host network.

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 could give attackers access to a home wi-fi network, 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>

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/>

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 Internet of Things, activated through apps, promises tremendous convenience to homeowners. But it may also prove irresistible to hackers. Carlos Gonzalez for The New York Times

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

iotworm.eyalro.net

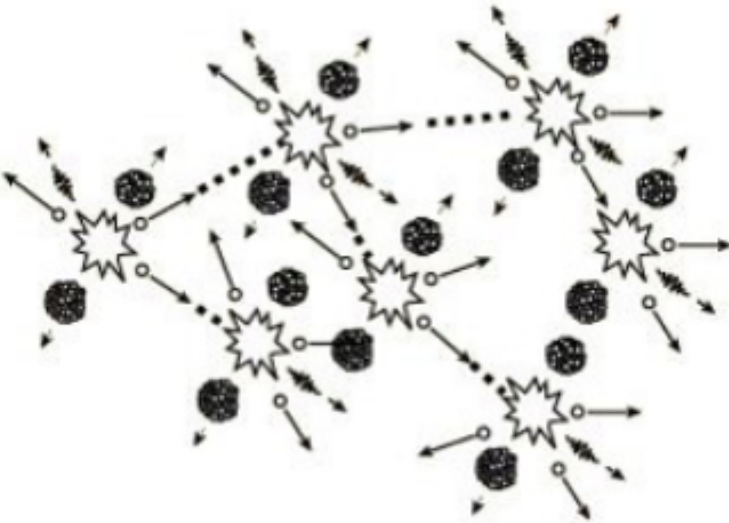
IoT Goes Nuclear - Creating a ZigBee Chain Reaction

IoT Goes Nuclear: Creating a ZigBee Chain Reaction

Eyal Ronen, Colin
O'Flynn, Adi Shamir
and Achi-Or
Weingarten

Creating an IoT worm

Within the next few years, billions of IoT devices will densely populate our cities. In this paper we describe a new type of threat in which adjacent IoT devices will infect each other with a worm that will spread explosively over large areas in a kind of nuclear chain reaction, provided that the density of compatible IoT devices exceeds a certain critical mass. In particular, we developed and verified such an infection using the popular Philips Hue smart lamps as a platform. The worm spreads by jumping directly from one lamp to its neighbors, using only their built-in ZigBee wireless connectivity and their physical proximity. The attack can start by plugging in a single infected bulb anywhere in the city, and then catastrophically spread everywhere within minutes, enabling the attacker to turn all the city lights on or off, permanently brick them, or exploit them in a massive DDOS attack. To demonstrate the risks involved, we use results from percolation theory to estimate the critical mass of installed devices for a typical city such as Paris whose area is about 105 square kilometers: The chain reaction will fizzle if there are fewer than about 15,000 randomly located smart



Vulnerability Note VU#884840

Animas OneTouch Ping insulin pump contains multiple vulnerabilities

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



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>

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 were managed by **Valtia**. The company who is in charge of managing the buildings overall operation and maintenance. According to CEO, Simo Rounela, in both cases the devices under attack were temporarily disabled.



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.

<http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter>

Botnets de Dispositivos IoT

Evolução sendo acompanhada em nossa rede de sensores desde 2013

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

Malware se propaga geralmente via Telnet

- protocolo para conexão remota, sem criptografia

Exploram 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

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

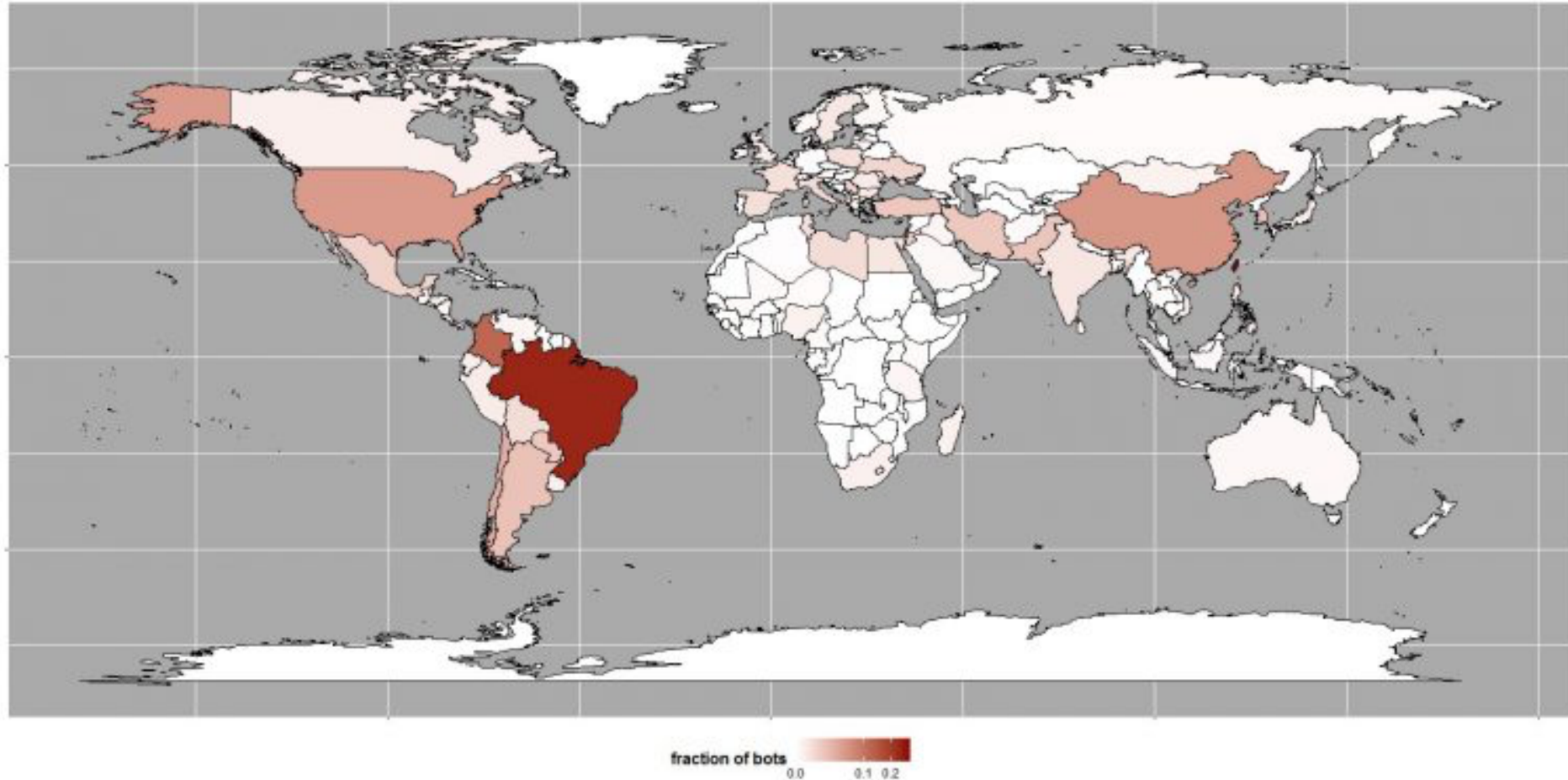
Original Release date: 13 Sep 2013 | Last revised: 04 Dec 2013



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.

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



Fonte: Estatísticas da distribuição global, Level3, 25 de agosto de 2016
<http://blog.level3.com/security/attack-of-things/>

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

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>

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>

Sierra Wireless: Roteadores 4G-WiFi também são afetados

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



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/

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

Malware waltzes up to admin panels with zero authentication

This appears to be a consequence of [TR-069](#) – aka the Customer-Premises Equipment WAN Management Protocol – which typically makes TCP/IP port 7547 available. ISPs use this protocol to manage the modems on their network. However, on vulnerable boxes, a TR-064-compatible server is running behind that port and thus accepts TR-064 commands that configure the hardware without authentication.

"The first issue, that of TR-064 being wide open to the internet, affects a whole host of other ISPs and vendors, and is, in fact, just as serious as the second one," said Martyn.

Martyn said he has confirmed that two routers provided by UK ISP TalkTalk are vulnerable – a ZyXEL modem and the D-Link DSL-3780. And he said that devices from T-Com/T-home (SpeedPort), MitraStar, Digicom, and Aztech are also at risk. In a [tweet](#) on Monday, Martyn said he has found 48 devices that are vulnerable to the TR-069/TR-064 issue.

28 Nov 2016 at 22:04, [Thomas Claburn](#)

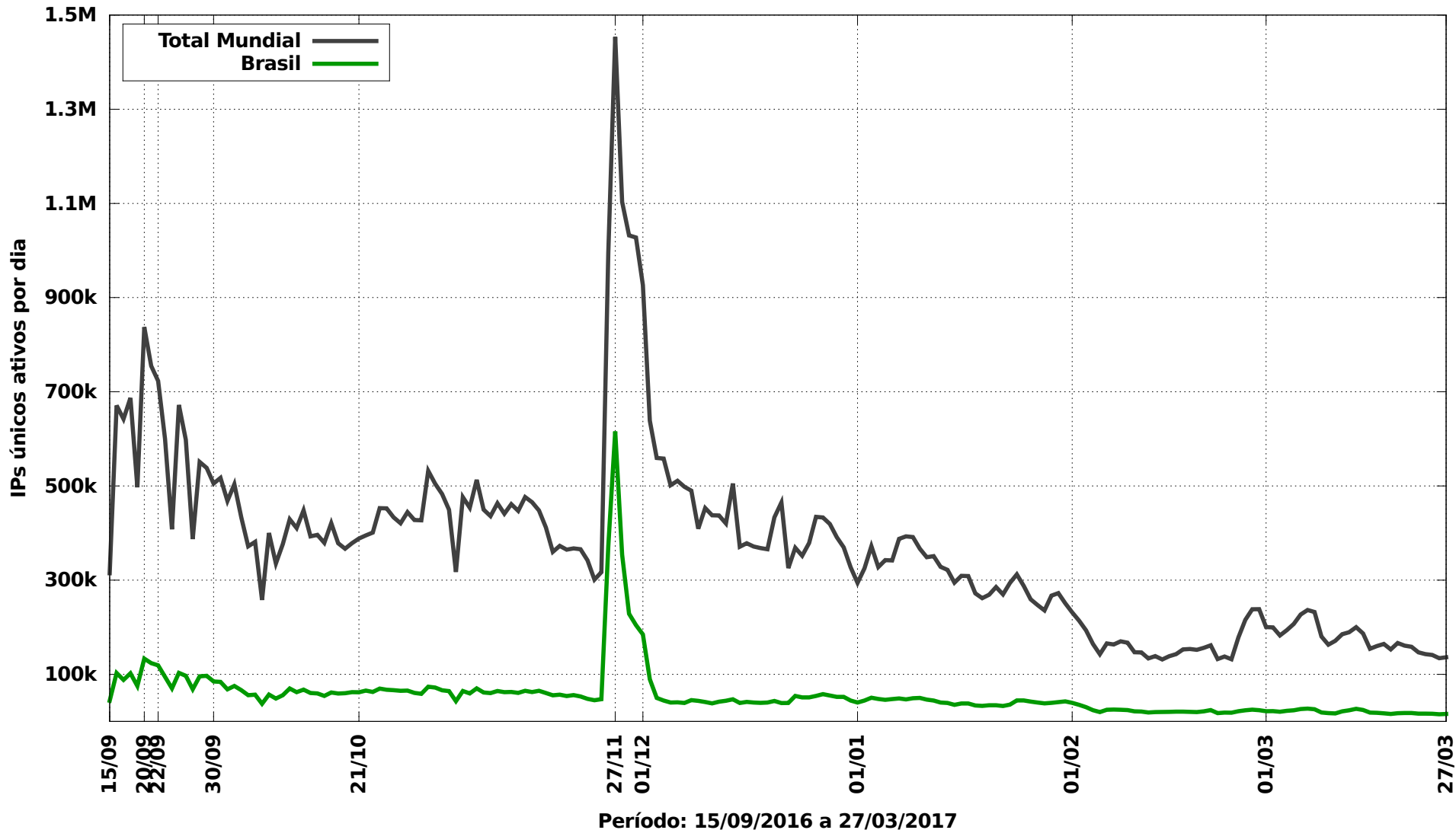


A widespread attack on the maintenance interfaces of broadband routers over the weekend has affected the telephony, television, and internet service of about 900,000 Deutsche Telekom customers in Germany.

http://www.theregister.co.uk/2016/11/28/router_flaw_exploited_in_massive_attack/

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

IPs Infectados com Mirai - todas as variantes: Total Mundial e Brasil



International

ISIS Wants to Enable Serial Killers by Hacking Surveillance Cameras

Terrorist group breaching security cameras to prepare for attacks

By **Joshua Philipp**, Epoch Times  |  November 1, 2016 AT 10:31 AM Last Updated: November 3, 2016 2:32 pm

The YouTube video ISIS was spreading alongside the online camera feeds shows how to take control of security cameras by using a basic cyberattack. The attack lets the terrorists change a camera's password, and gain deeper access to its system controls. Using this method, they can then control the cameras remotely.

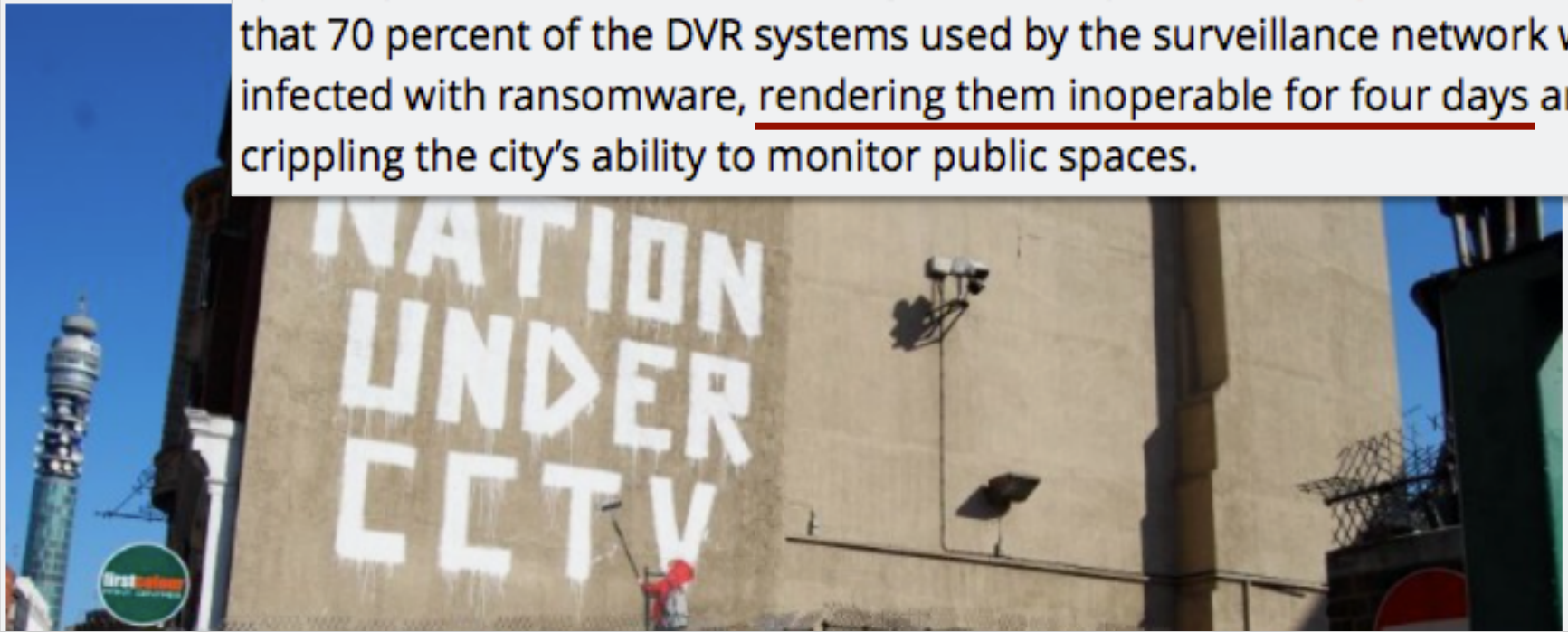
<http://www.theepochtimes.com/n3/2179764-isis-wants-to-enable-serial-killers-by-manipulating-surveillance-cameras/>

DC police surveillance cameras were infected with ransomware before inauguration

Malware seized 70 percent of DC police DVRs a week before Trump's inauguration.

SEAN GALLAGHER - 1/30/2017, 5:12 PM

system just one week before Inauguration Day. *The Washington Post* reports that 70 percent of the DVR systems used by the surveillance network were infected with ransomware, rendering them inoperable for four days and crippling the city's ability to monitor public spaces.



<https://arstechnica.com/security/2017/01/dc-police-surveillance-cameras-were-infected-with-ransomware-before-inauguration/>

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The top and bottom sections of the slide feature this pattern, while the middle section is a solid light gray gradient.

Desafios para Melhorar o Cenário

cert.br nic.br cgi.br

Vulnerabilidades em IoT: O que chama mais atenção

Segurança não é prioridade

- mesmo em dispositivos de segurança!

Raríssimos consideram ciclo de atualizações de segurança

Todos repetem os erros do passado

- falta de autenticação
 - quando tem, são senhas fracas
- protocolos sem criptografia
- “*backdoors*” dos fabricantes são a norma
 - usualmente senhas padrão, que não podem ser alteradas, nem as contas desabilitadas

Como melhorar o cenário

Solução depende de diversas camadas

- desenvolvedores e fabricantes
- usuários e administradores de sistemas

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

- deve ser possível atualizar dispositivos IoT
- 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

Usuários e Administradores de Sistemas (2/2)

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

Resumindo:

Cabe a Vocês Demandar Segurança!

Não assumam que “é seguro” só porque uma empresa de segurança (física?) disse que é

- Ex. câmeras de segurança, monitores de bebês, etc

Assuma que o fabricante/desenvolvedor:

- não pensou em ataques pela Internet
- não pensou em *update* de *firmware*
 - e se pensou, permite *update* automático sem verificação de autenticidade
- não tem pessoal especializado em segurança
 - ex: que entenda de autenticação, desenvolvimento seguro, cripto, etc
- vai reutilizar código vulnerável

Obrigada

www.cert.br

© cristine@cert.br

© @certbr

28 de março de 2017

nic.br cgi.br

www.nic.br | www.cgi.br