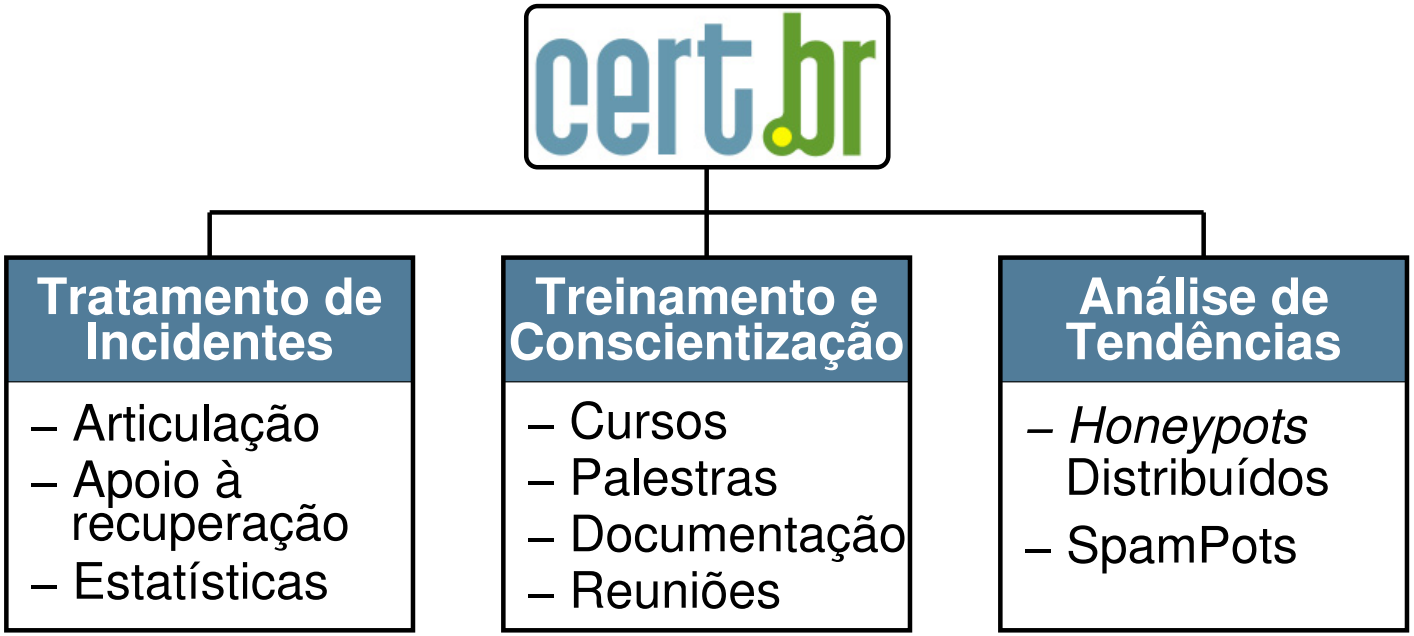
nic.br cgi.br | cert.br

1° Semana da Computação
Rio das Ostras, RJ
04 de maio de 2016

Segurança e IoT: Desafios e Expectativas

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

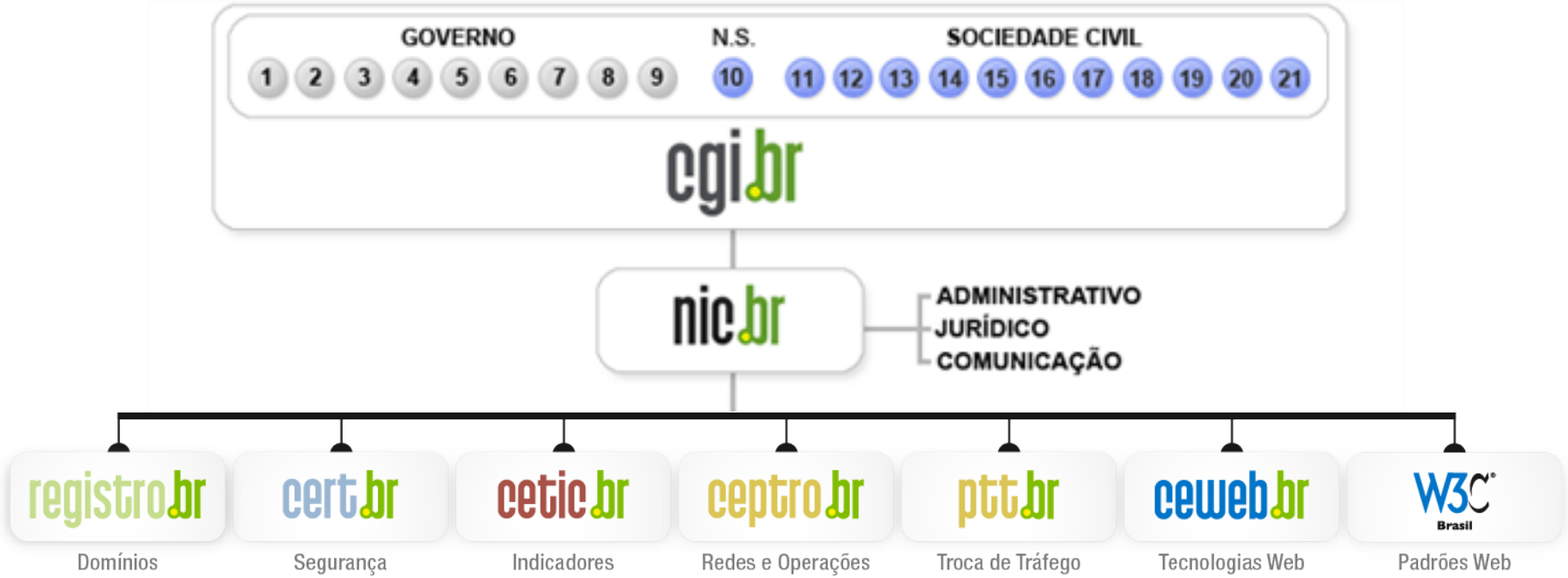
The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Comitê Gestor da Internet no Brasil – CGI.br

Entidade multissetorial, criada em 1995, responsável por coordenar e integrar as iniciativas e serviços da Internet no País.

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

http://www.cgi.br/sobre/

Agenda

- **Internet das Coisas**

- **Responder questões sobre IoT e segurança**
  - Nova tecnologia?
  - Novos riscos?
  - Novos desafios?

- **Referências**

Internet das Coisas
Nova tecnologia?

cert.br nic.br cgi.br

Computação Ubíqua

- **Mark Weiser, em 1988**
- **Oposto da “realidade virtual”**
  - **pessoas colocadas em realidade gerada por computadores**
- **Computador se integra a vida das pessoas**
  - **utilizado sem ser notado, tecnologia “calma”**
  - **pano de fundo de nossas vidas**
- **Ainda sem recursos disponíveis na época para ser usada**

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.”

The Computer for the 21st Century

http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html

Internet das Coisas – Surgimento

- ***Internet of Things*** **(IoT),** ***Internet of Everything*** **(IoE)**
- **Kevin Ashton, em 1999**
  - apresentação para executivos sobre como facilitar a logística da cadeia de produção usando RFID
- **Ainda com poucos recursos para ser usada**

"We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory."

That 'Internet of Things' Thing
In the real world, things matter more than ideas

http://www.rfidjournal.com/articles/view?4986

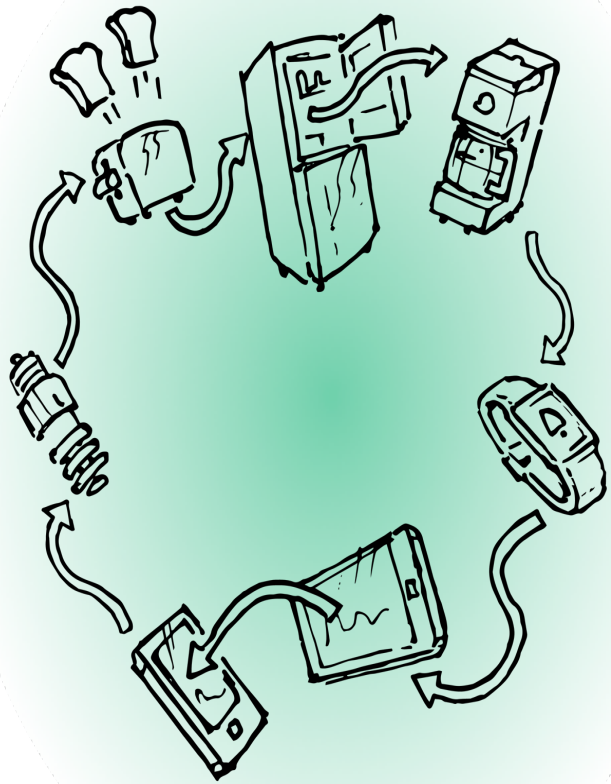
Internet das Coisas – Atualidade

“... is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity...”

Wikipedia

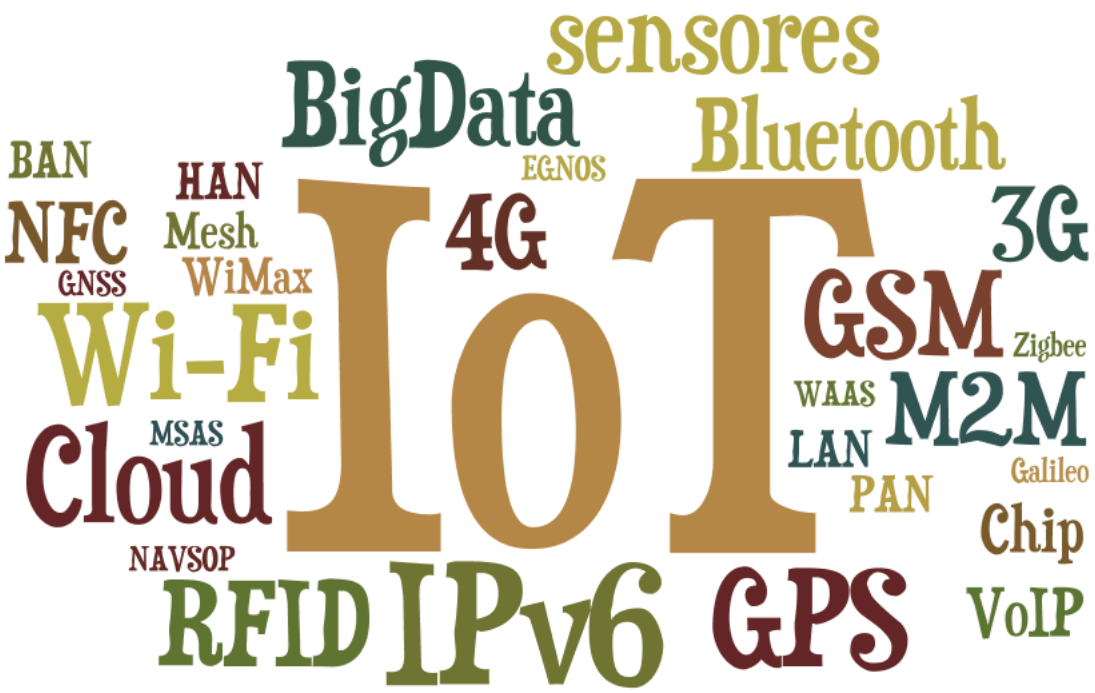
“...The Internet of Things extends internet connectivity beyond traditional devices like desktop and laptop computers, smartphones and tablets to a diverse range of devices and everyday things...”

Webopedia



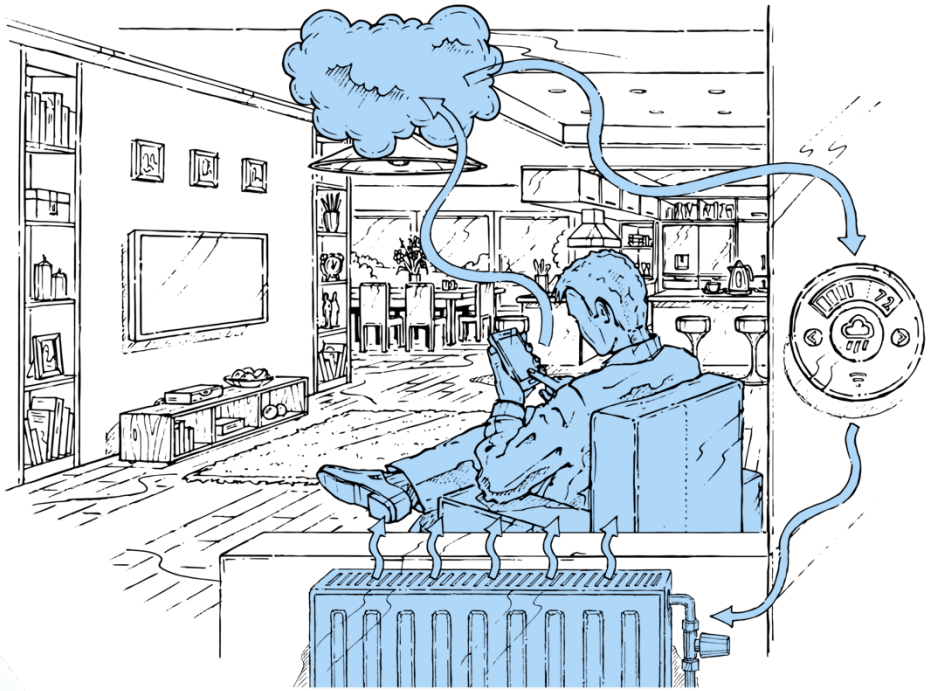
Internet das Coisas – Atualidade

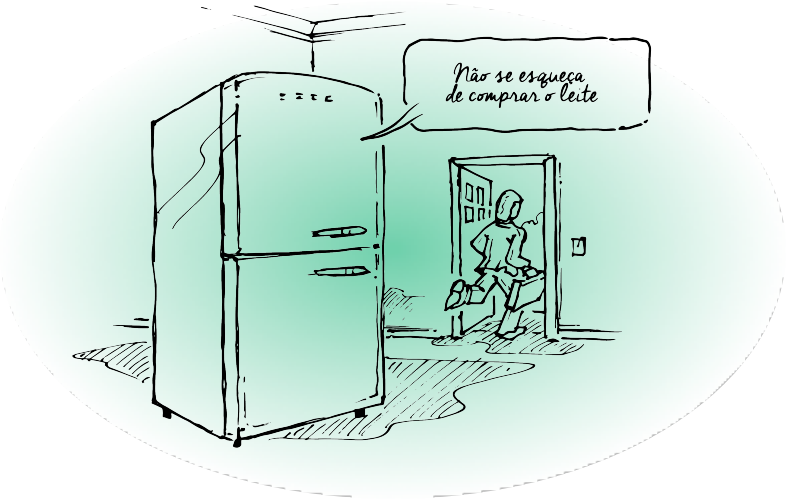
- **As coisas já estão conectadas**
  - sistemas complexos e completos
    - sistema operacional, aplicações Web, permitem acesso remoto, etc
    - múltiplas tecnologias



Internet das Coisas – Usos

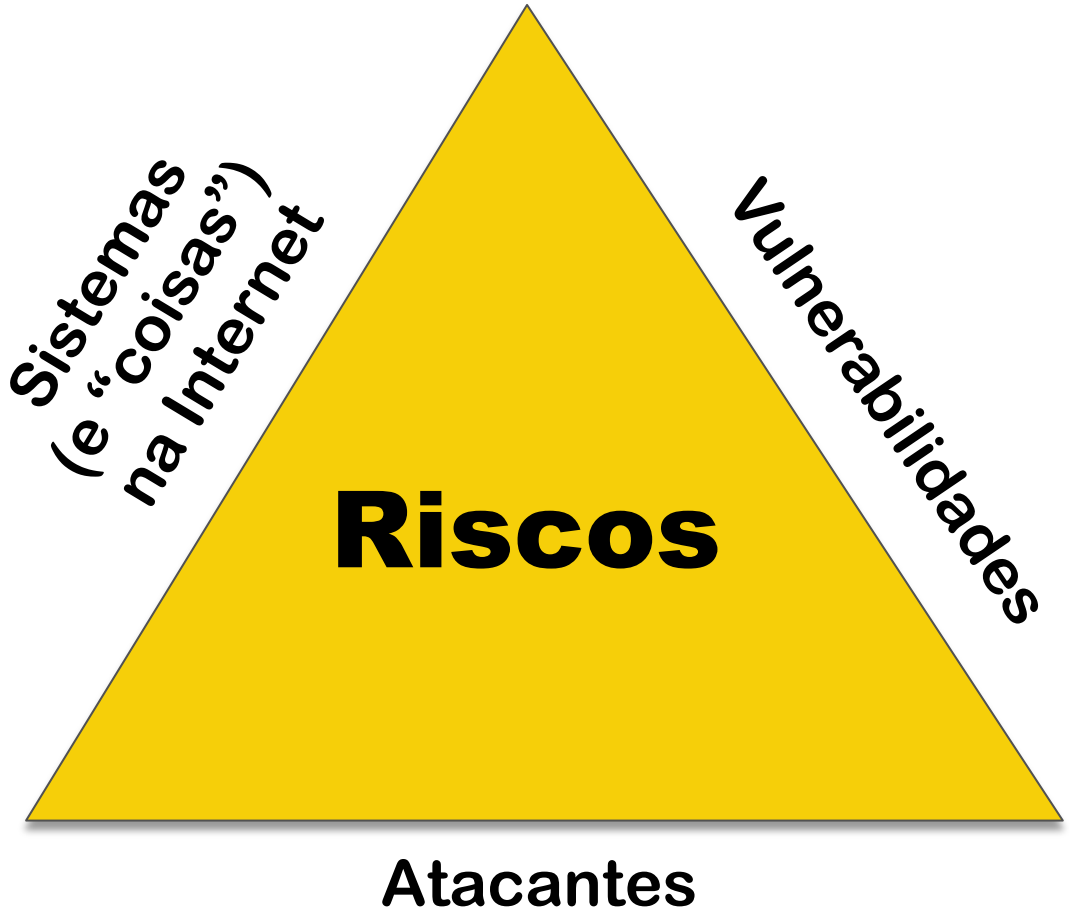
- **Casas inteligentes**
- **Cidades inteligentes**
- **Carros conectados**
- **Equipamentos médicos**
- **Industria 4.0**
- ***Wearables***





Novos riscos?

cert.br nic.br cgi.br


Sistemas
(e "coisas")
na Internet
Vulnerabilidades
Riscos
Atacantes

Atacantes

- **criminosos**
- **espionagem industrial**
- **governos**
- **vândalos**
- **pessoas que querem diversão**

Vulnerabilidades

- **projeto sem levar em conta segurança**
- **sistemas desatualizados**
  - defasagem de tempo entre ser “fabricado” e chegar ao cliente
- **defeitos de *software/firmware***
- **falhas de configuração**
- **falta de proteção de dados**
- **uso inadequado**
- **contas:**
  - sem senhas
  - com senhas fracas ou *default*
  - de serviço (*backdoors*)
  - com acesso remoto

Riscos

- violação de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- perda de confiança na tecnologia
- indisponibilidade de serviços críticos
- participação em golpes
- propagação de códigos maliciosos
- envio de *spam*
- risco de morte

Exemplos

- **Lâmpadas Phillips Hue LED**
  - criptografia fraca permite descobrir senha do Wi-Fi
  - vulnerabilidades permitem controlar remotamente
- **Samsung**
  - TVs mandam todo o som ambiente para sede
  - vulnerabilidades no SmartThings, permitem abrir portas e gerar falsos alarmes de fumaça
- **TVs da LG**
  - enviam nomes de arquivos, filmes, inclusive dos drives de rede, que são ativamente procurados pela TV
- **Carros da Fiat Chrysler**
  - permitindo controle do veículo via 3G/4G
  - via vulnerabilidades do sistema de entretenimento Uconnect

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.

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities | ICS-CERT

https ics-cert.us-cert.gov/advisories/ICSA-15-161-01 Reader

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]

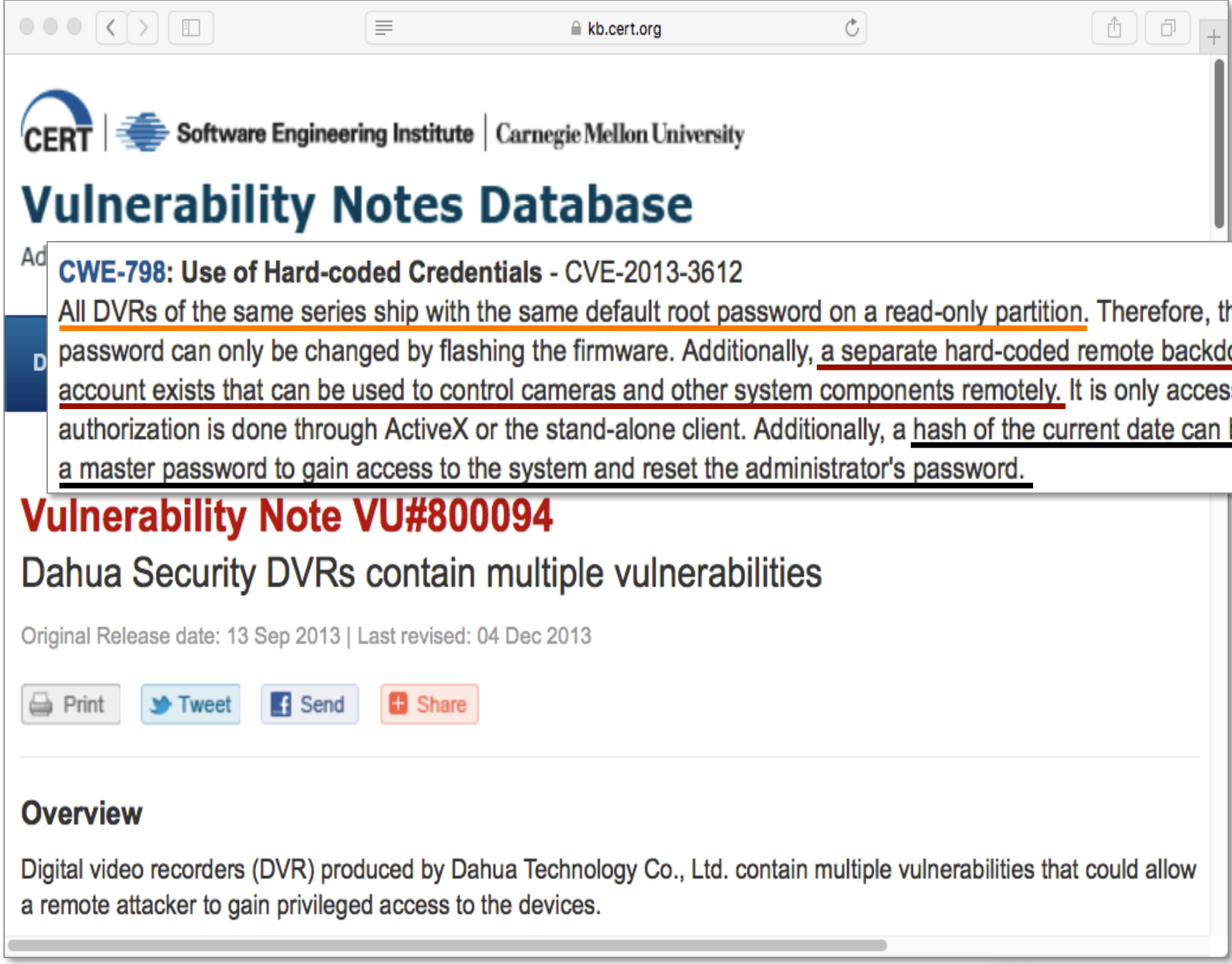
IMPROPER AUTHORIZATION[e]

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 unauthorized devices on the host network.


kb.cert.org
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
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.

kb.cert.org

Dahua Security DVRs contain multiple vulnerabilities

Date Notified: 09 Jul 2013 Vendor Information Hel

Statement Date:

Date Updated: 04 Dec 2013

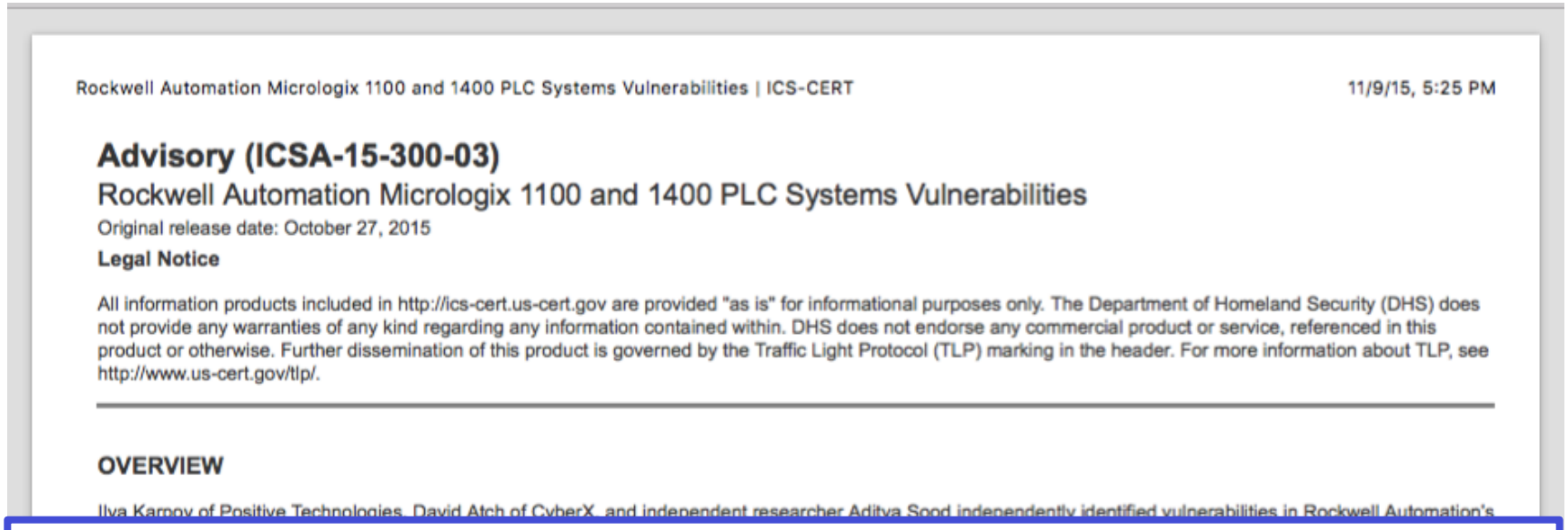
Status

Unknown. If you are the vendor named above, please contact us to update your status.

Vendor Statement

Five separate attempts to contact Dahua were made, but the vendor failed to respond.

After publishing, Dahua disputes CVE-2013-3612, CVE-2013-3613, and CVE-2013-3614. Specifically, Dahua states that the telnet port cannot be mapped via UPnP. Dahua also states that the six character password requirement cannot be brute forced due to an account lockout mechanism after three unsuccessful login attempts. Lastly, Dahua states that the master password in CVE-2013-3612 can only be used by a local user.



Rockwell Automation Micrologix 1100 and 1400 PLC Systems Vulnerabilities | ICS-CERT 11/9/15, 5:25 PM

Advisory (ICSA-15-300-03)

Rockwell Automation Micrologix 1100 and 1400 PLC Systems Vulnerabilities

Original release date: October 27, 2015

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

Ilya Karpov of Positive Technologies, David Atch of CyberX, and independent researcher Aditya Sood independently identified vulnerabilities in Rockwell Automation's

VULNERABILITY CHARACTERIZATION

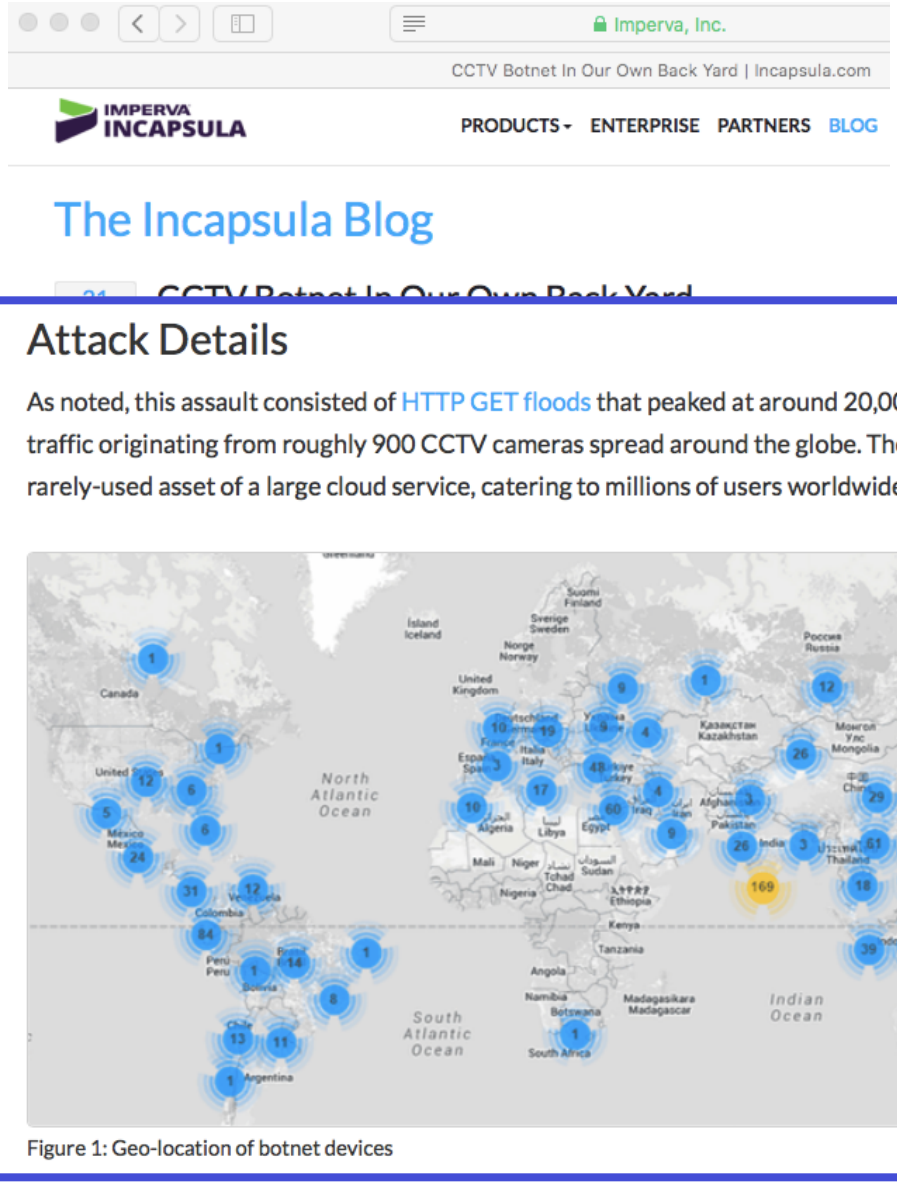
STACK-BASED BUFFER OVERFLOW
IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER
UNRESTRICTED UPLOAD OF FILE WITH DANGEROUS TYPE
CROSS-SITE SCRIPTING
SQL INJECTION

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

Fonte: https://ics-cert.us-cert.gov/advisories/ICSA-15-300-03



Fonte: https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html

Ohio couple terrorized after hacker takes over baby-monitoring camera

Heather and Adam Schreck were terrified when they heard an unknown male voice in their Cincinnati home at midnight shouting 'Wake up, baby!' Adam rushed to baby Emma's room to make sure she was OK, but it was then that the family discovered their Foscam baby-monitoring camera had been hacked and was being controlled by a virtual intruder.

BY MELANIE GREENWOOD / NEW YORK DAILY NEWS / Monday, April 28, 2014, 9:52 AM

Share 1355 Tweet

SHARE THIS URL

nydn.us/1rwYG2C

Wake Up, baby

http://www.nydailynews.com/news/national/baby-monitoring-camera-hacked-taunts-family-article-1.1771399

Shodan: The IoT search engine for watching sleeping kids and bedroom antics

"Internet of Things" security is hilariously broken and getting worse

Shodan search engine is only the latest reminder of why we need to fix IoT security.

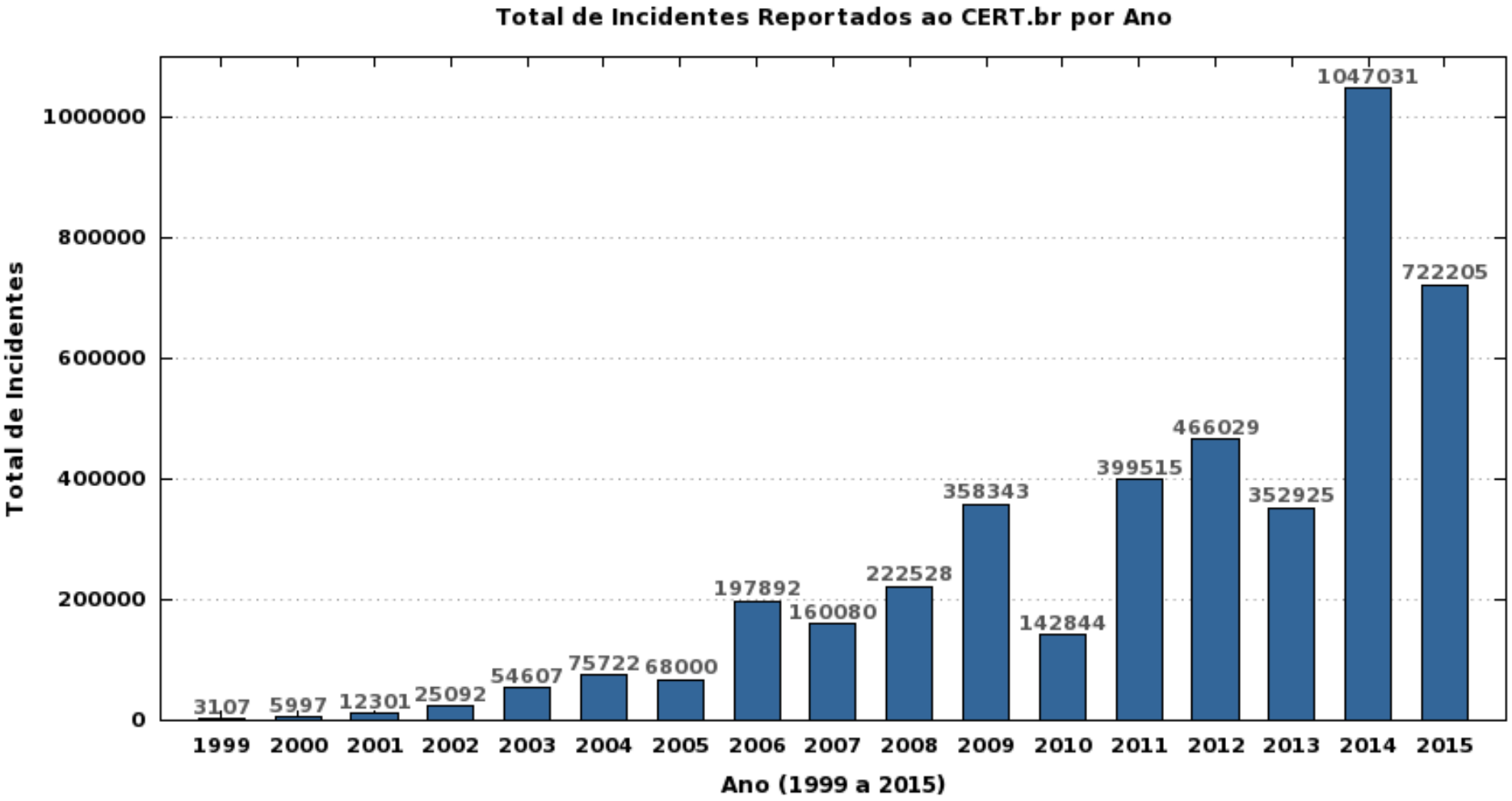
The cameras are vulnerable because they use the Real Time Streaming Protocol (RTSP, port 554) to share video but have no password authentication in place. The image feed is available to paid Shodan members at images.shodan.io. Free Shodan accounts can also search using the filter port:554 has_screenshot:true.

http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/
http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/

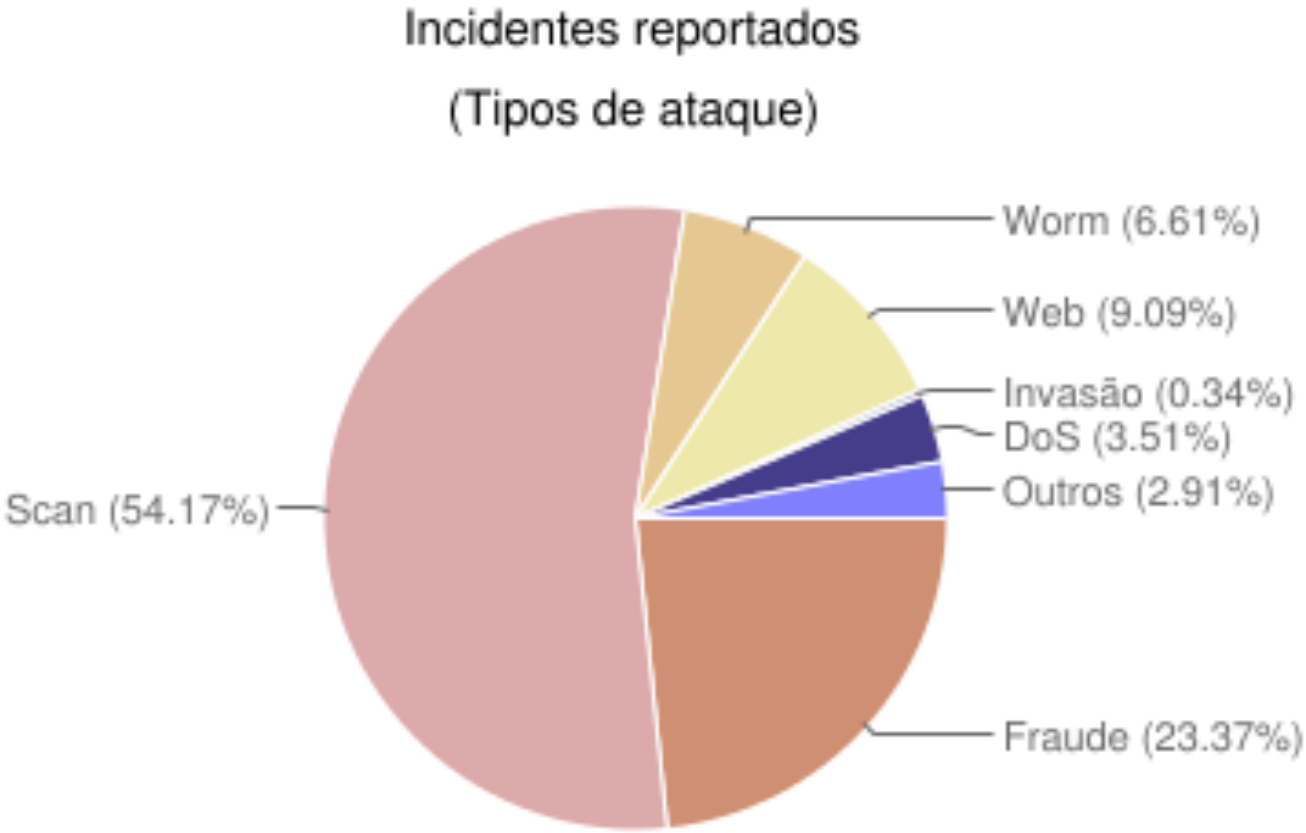
Estatísticas gerais de incidentes

cert.br nic.br cgi.br

Estatísticas CERT.br – 1999 a 2015

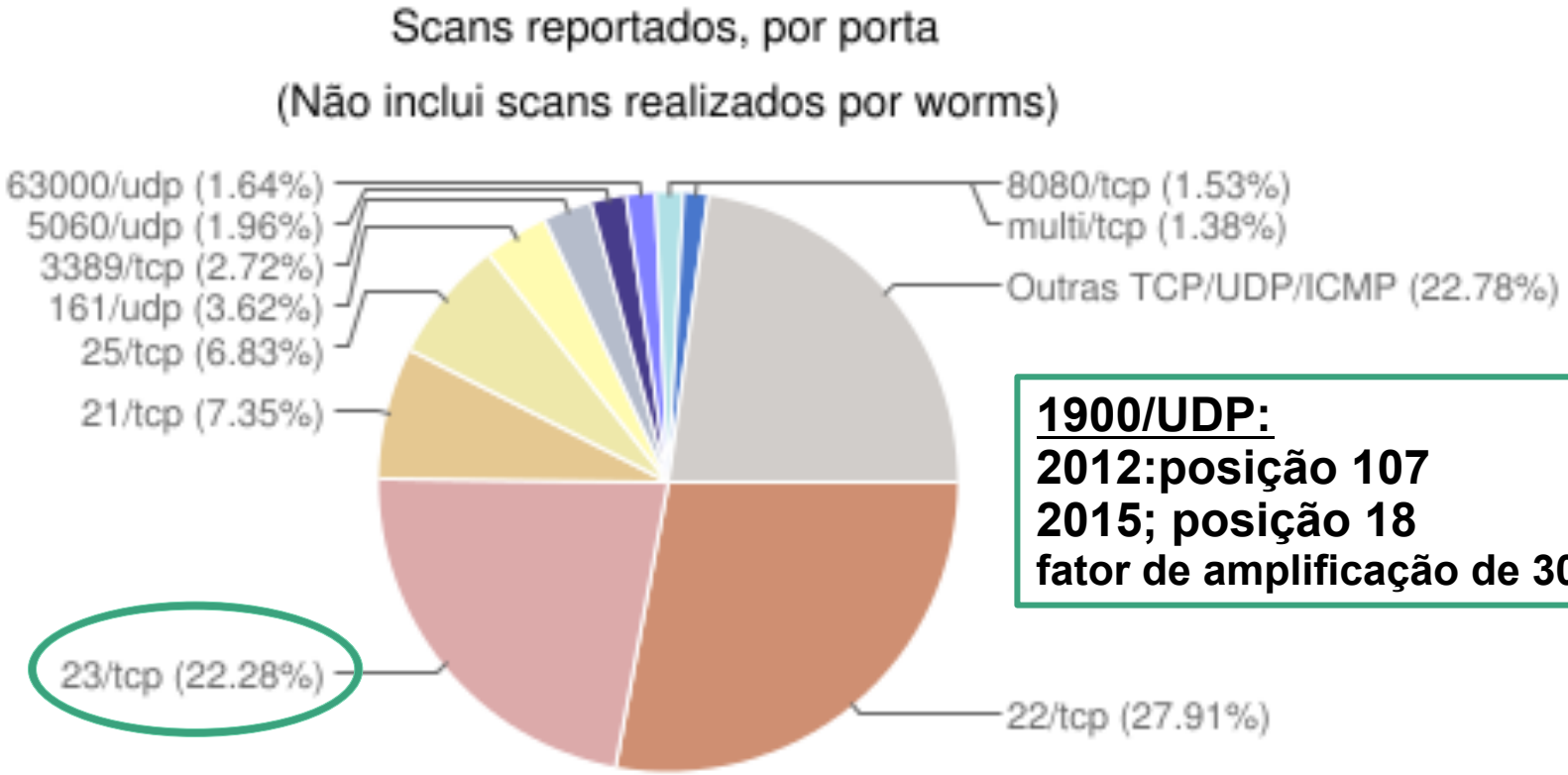


Estatísticas CERT.br – 2015



***scan*: aumento de 48% em relação a 2014**

Estatísticas CERT.br – 2015



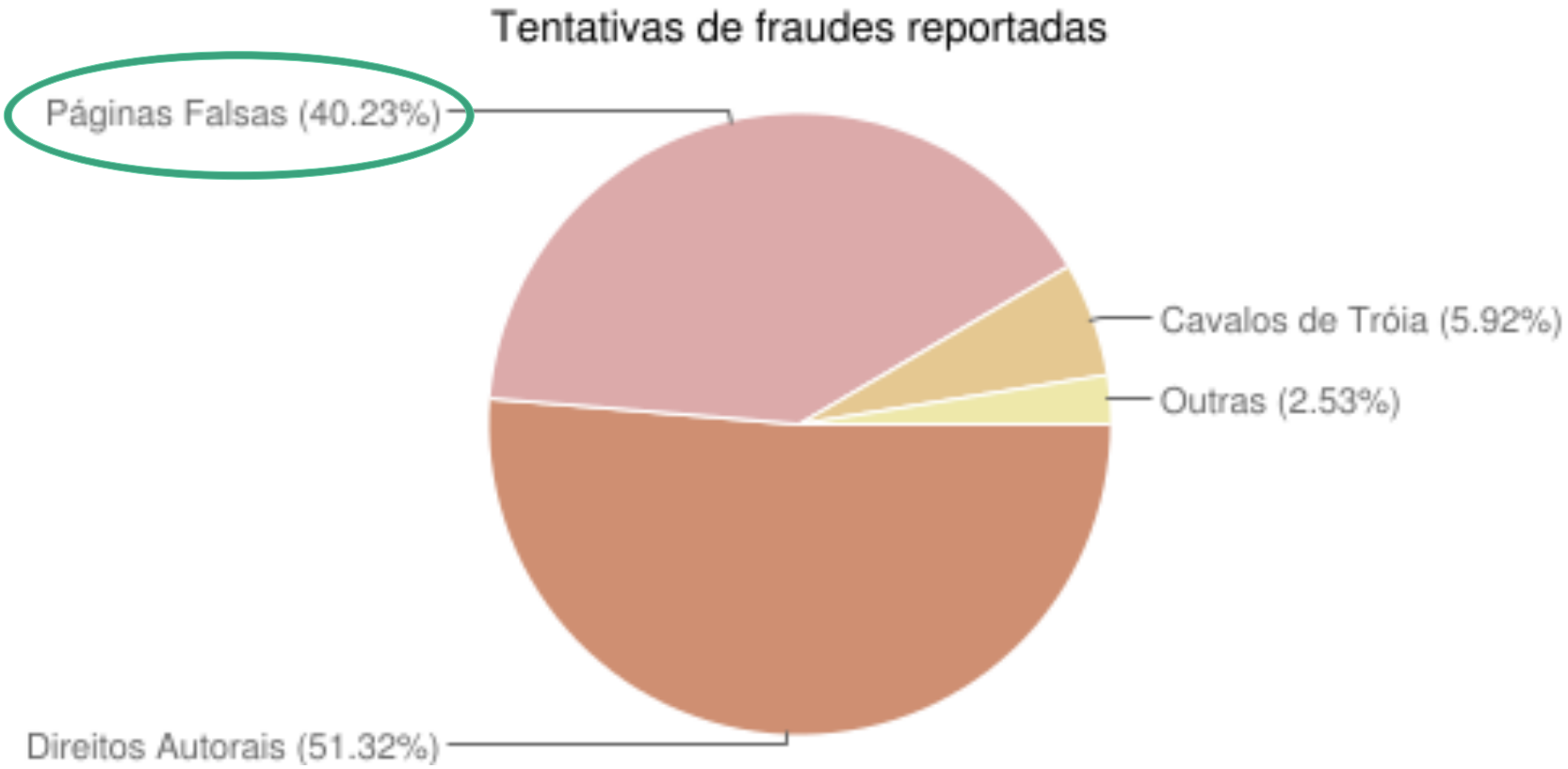
1900/UDP:
2012:posição 107
2015; posição 18
fator de amplificação de 30.8

23/TCP: em 2014 era 10%

Report: IoT-Connected Devices Leading to Rise in SSDP-based Reflection Attacks

http://www.darkreading.com/attacks-breaches/report-iot-connected-devices-leading-to-rise-in-ssdp-based-reflection-attacks-/d/d-id/1320149

Estatísticas CERT.br – 2015



Novos desafios?

cert.br nic.br cgi.br

Desafios (1/5)

- **Tratamento de incidentes**
  - dificuldade de explicar e de entender o problema
  - o que temos ouvido no dia-a-dia:
    - “Isto é apenas um(a) [_____]”
    - “Não, a gente não tem Internet aqui...”
    - “Esse dispositivo não é minha responsabilidade...”

Desafios (2/5)

- **Segurança deve ser nativa**
  - não deve ser opcional
  - requisitos de segurança devem ser considerados desde o projeto
  - desenvolvimento seguro
    - falta de desenvolvedores treinados
- **Custos de segurança**
  - segurança não é prioridade
- **Como incluir segurança na cadeia de produção?**
  - tempo de projeto X tempo de chegar ao cliente

Desafios (3/5)

- **Definição e normatização de responsabilidades**
  - quem lança as correções?
  - quem aplica as correções?
  - quem e como os clientes contatam as empresas?

- **Políticas de atualização inexistentes**
  - a política em geral é “comprar outro”
  - vale a pena atualizar equipamentos muito baratos?
  - tempo de suporte X tempo de vida útil do equipamento

- **Interoperabilidade entre os equipamentos**
  - Web das Coisas

Desafios (4/5)

- **Proteção de dados**
  - responsabilidades
  - assimetria de acesso entre empresas e consumidores
    - planos de saúde
    - seguradoras de veículos
    - compras em geral
- **Comportamento autônomo das coisas**
  - difícil adquirir equipamentos sem essas tecnologias
- **Tudo tem que estar conectado**
  - porque é possível conectar não significa que tem que estar

Desafios (5/5)

- **Não confundir segurança física com computacional**
  - não assumir que “é seguro” só porque uma empresa de segurança (física?) disse que é
- **Usuários não são especialistas**

Mesmos velhos problemas

telnet, senha *default*, falta de atualização, erros de programação, etc

Referências

cert.br nic.br cgi.br

Referências

- **A Internet das coisas, explicada pelo NIC.br**
  - https://youtu.be/jlkvzcG1UMk
- **Segurança em um Mundo Conectado (IoT x Segurança)**
  - http://www.ricardokleber.com/palestras/2016_01_28_-_CPBR9_-_Seguranca_x_IoT.pdf
  - http://segurancaderedes.com.br/assista-ao-vivo-a-palestra-seguranca-e-iot-na-cpbr9/
- **Vulnerabilidades e Ataques na Internet das Coisas**
  - https://youtu.be/fSzBRP1rWrI
- ***The OWASP Top 10 IoT Vulnerabilities***
  - *https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf*

Obrigada

www.cert.br

miriam@cert.br

@certbr

04 de maio de 2016

nic.br cgi.br

www.nic.br | www.cgi.br