FEBRABAN
Federação Brasileira de Bancos

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

Cristine Hoepers, D.Sc.
Gerente Geral – CERT.br/NIC.br

A Internet das Coisas

- **"... 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*

O que temos ouvido no dia-a-dia de tratamento de incidentes...

“Isto é apenas um(a) [_____]”

“Não, a gente não tem Internet aqui...”

“Esse dispositivo não é minha responsabilidade...”

Sistemas (e “coisas”) na Internet

- indisponibilidade de serviços
- perda de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- perda de confiança na tecnologia

Riscos

Atacantes

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

- projeto sem levar em conta segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

As “coisas” já estão conectadas

- **carros, lâmpadas, TVs, eletrodomésticos, equipamentos médicos**
- **são sistemas complexos e completos (tem um sistema operacional, aplicações Web, permitem acesso remoto, etc)**

Mas não estão sendo tomados cuidados de segurança no projeto, implementação e adoção, vide:

- **Lâmpadas *Phillips Hue LED* (cripto fraca permite descobrir senha do wi-fi; vulnerabilidades permitem controlar remotamente)**
- **TVs Samsumg mandam todo o som ambiente para sede; 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**
- **Aviões potencialmente vulneráveis via sistemas de entretenimento**
- **Dispositivos médicos**

Infusion Pumps

www.hospira.com/en/products_and_services/infusion_pumps

Reader

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.

Contact Hospira

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

Statement Date:

Date Updated: 04 Dec 2013

Vendor Information Hel

Status

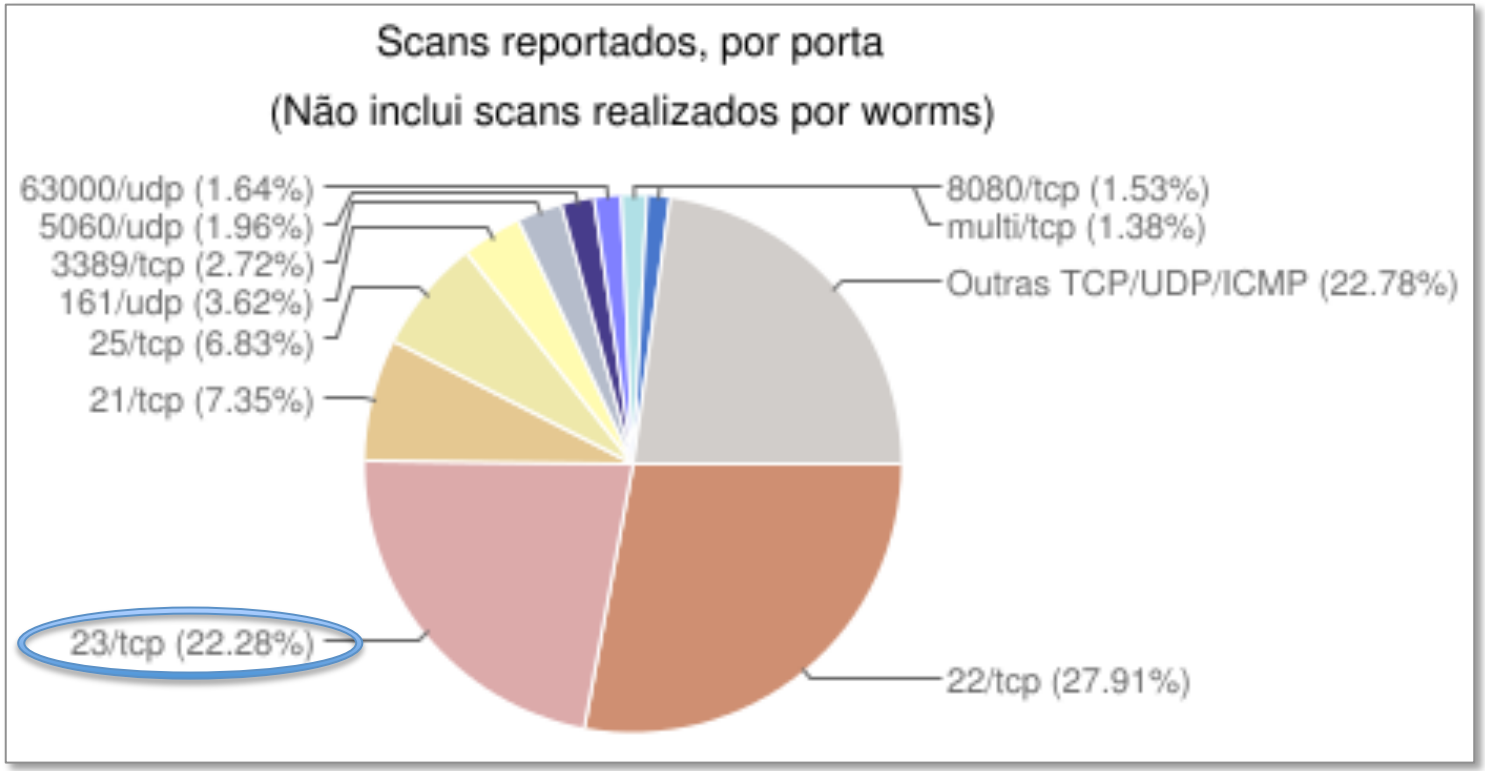
Unknown. If you are the vendor named above, please contact us to update your status.

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.

Estatísticas 2015 - varreduras



http://www.cert.br/stats/incidentes/

Incidentes Recentes em Sistemas de Câmeras de Segurança

- **Phishing hospedado em um CCTV/DVR**
  - **"*Mas aqui não tem Internet*"**
- **CCTV/DVR utilizado para desferir ataques DDoS**
  - **embora sendo de "fabricante nacional", possuía as vulnerabilidades do documento visto anteriormente, incluindo porta TELNET com senha padrão:**

    Vulnerability Note VU#800094

    Dahua Security DVRs contain multiple vulnerabilities

    http://www.kb.cert.org/vuls/id/800094

Incidentes Envolvendo "*modems*" e roteadores banda larga (CPEs)

CPEs são vistos como "coisas"

- **ninguém assume responsabilidade por configuração e atualização**

Comprometidos

- **via força bruta de telnet**
  - **via rede ou via *malware* nos computadores das vítimas**
- **explorando vulnerabilidades**
- **através de *iFrames* com *JavaScripts* maliciosos**
  - **colocados em sites comprometidos, blogs, etc**

Objetivos dos ataques

- **alterar a configuração de DNS**
  - **para fazer fraudes ou infectar os usuários**

Tendências de [in]Segurança em IoT

- **P&D não vai se preocupar com segurança**
- **prioridade é baixo custo**
  - **de hardware**
  - **de contratação de desenvolvedores**
- **políticas de atualização são inexistentes**
  - **mesmo para CPEs, a política em geral é "comprar outro"**
  - **em casos como o das TVs Digitais com Ginga, os desenvolvedores são taxativos: "não dá pra fazer update 'pelo ar' "**
    - **mas cogita-se ter serviços como internet banking via o espectro alocado para a TV**

Cabe a Vocês Demandar Segurança

- **Não assuma 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!

Cristine Hoepers, D.Sc.

Email: cristine@cert.br
http://www.cert.br/