nic.br cgi.br

20 anos cert.br

VII Fórum da Internet no Brasil

Rio de Janeiro, RJ

15 de novembro de 2017

Segurança, Estabilidade e Resiliência da Internet para um Ecossistema Saudável

Dra. Cristine Hoepers
Gerente Geral, CERT.br
cristine@cert.br

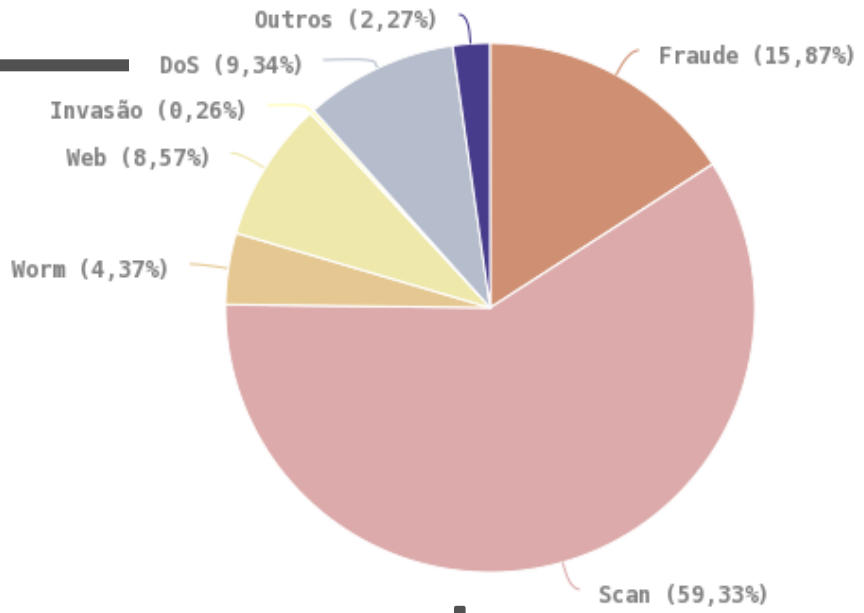
cert.br nic.br cgi.br

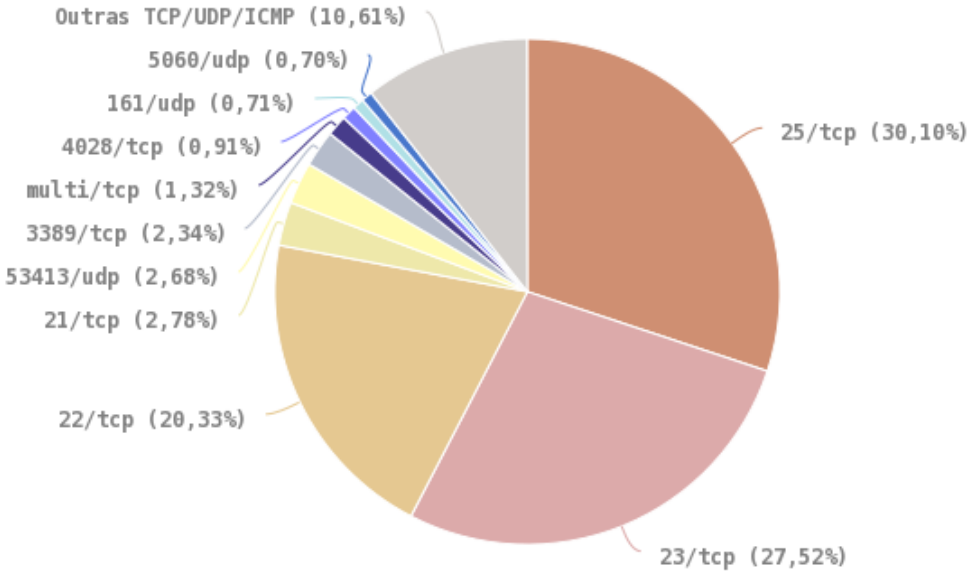
Cenário Nacional

Incidentes Notificados – Destaques em 2016

DDoS – aumento de 138%

- **300Gbps é o novo "normal"**
  - Até 1Tbps contra alguns alvos
- **Tipos mais frequentes**
  - *botnets* IoT
  - amplificação





Scan

- **Portas 22 e 23:** força bruta de senhas de servidores e de IoT
- **Porta 25:** força bruta de senhas de *e-mail*

Atividades nos *Honeypots* Distribuídos: **Serviços mais Visados**

Força bruta de senhas (ataque usado por *malwares* de IoT e para invasão de servidores e roteadores):

- Telnet (23/TCP)
- SSH (22/TCP)
- RDP (3389/TCP)
- POP3 (110/TCP)
- Outras portas TCP (2323, 23231, 2222)

Protocolos explorados pela *botnet* IoT Mirai, na variante para CPEs (*modems* e roteadores de banda larga)

- TCP: 7547, 5555, 37777, 6789, 81

Busca por protocolos que permitam amplificação

- UDP: DNS, NTP, SSDP, SNMP, Chargen, Netbios, Quotd, mDNS, LDAP

Total de Notificações de IPs com Serviços Mal Configurados que Permitem Amplificação

Número de Sistemas Autônomos e Endereços IP únicos, alocados ao Brasil, notificados pelo CERT.br em agosto e setembro de 2017

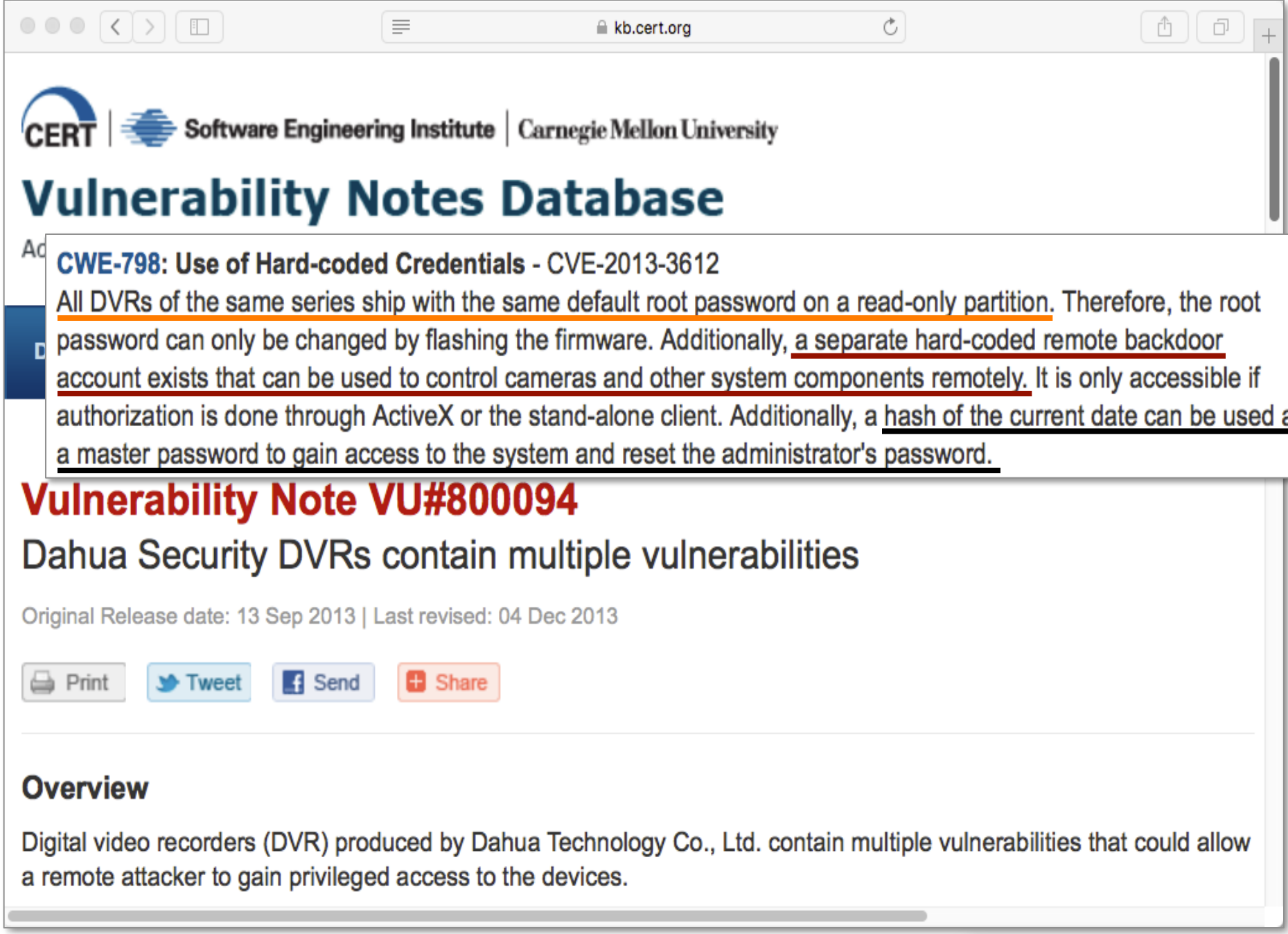
	Agosto		Setembro	
	ASNs	IPs	ASNs	IPs
SNMP	2.018	554.457	1.791	406.015
DNS	2.347	72.677	2.307	62.283
NTP	872	108.168	800	89.603
SSDP	891	27.209	⦸	⦸

Legenda:

⦸ não foi realizada notificação desta categoria no referido mês

Artigo do ShadowServer sobre os testes de amplificadores:
http://blog.shadowserver.org/2014/03/28/the-scannings-will-continue-until-the-internet-improves/

Por que esses abusos são possíveis?


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.

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)

Hospira Plum A+ and Symbiq Infusion Systems Vu

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
be exploited to allow execution of arbitrary code on the device. This v
However, acting out of an abundance of caution, ICS-CERT is includi
providers' awareness, so that additional monitoring and controls can b

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2 b
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.

Infusion Pumps

www.hospira.com/en/products_and_services/infusion_pumps

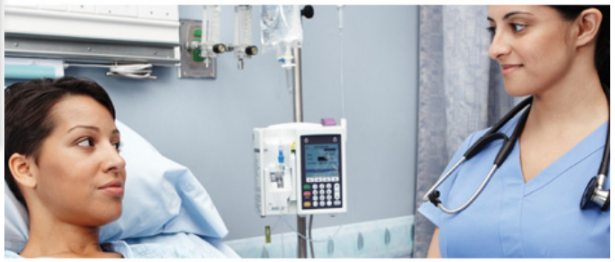
Reader

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:

Contact Hospira



PLUM 360™ INFUSION SYSTEM

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

kb.cert.org

Vulnerability Note VU#778696

Netgear D6000 and D3600 contain hard-coded cryptographic keys and are vulnerable to authentication bypass

Original Release date: 10 Jun 2016 | Last revised: 01 Jul 2016

Print Tweet Send Share

Overview

The Netgear D6000 and D3600 routers are vulnerable to authentication bypass and contain hard-coded cryptographic keys embedded in their firmware.

Description

CWE-321: Use of Hard-coded Cryptographic Key -- CVE-2015-8288

The firmware for these devices contains a hard-coded RSA private key, as well as a hard-coded X.509 certificate and key. An attacker with knowledge of these keys could gain administrator access to the device, implement man-in-the-middle attacks, or decrypt passively captured packets.

CWE-288: Authentication Bypass Using an Alternate Path or Channel -- CVE-2015-8289

A remote attacker able to access the `/cgi-bin/passrec.asp` password recovery page may be able to view the administrator password in clear text by opening the source code of above page.

Roteadores 4G-WiFi Utilizados em Infraestruturas Críticas

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/

Pontos em Comum em Indústrias tão Diferentes: **Velhos Problemas**

Muitas vulnerabilidades

Preocupação zero com segurança

- "alguém" fará a segurança depois...
- maioria não prevê atualização de *firmware*

Falta de Autenticação

- para conectar e receber comandos
- para fazer atualizações

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*?

“Dificilmente existirá alguma coisa nesse mundo que alguém não possa

fazer um pouco pior e

vender um pouco mais barato,

e as pessoas que considerarem somente preço são as merecidas vítimas.”

– John Ruskin
(1819–1900)

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

COMPLETELY BROKEN —

Millions of high-security crypto keys crippled by newly discovered flaw

Factorization weakness lets attackers impersonate key holders and decrypt their data.

DAN GOODIN - 10/16/2017, 9:00 AM

The flaw resides in the Infineon-developed RSA Library version v1.02.013, specifically within an algorithm it implements for RSA primes generation. The library allows people to generate keys

This is the second time in four years that a major crypto flaw has been found hitting a crypto scheme that has passed rigorous certification tests. In 2013,

Enlarge / 750,000 Estonian cards that look like this use a 2048-bit RSA key that can be factored in a matter of days.

"... the real security challenge is not the mathematics of cryptosystems; it is engineering, specifically the design and implementation of complex software systems."

– *Keys Under Doormats,* Abelson et. al

http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

Breves Considerações sobre Acesso Excepcional: **Possíveis Consequências Não Intencionais**

Cria-se uma nova superfície de ataque

Retrocede-se a segurança dos sistemas

- ex.: inviabiliza o uso da técnica de *Forward Secrecy*

Incentiva-se o crime organizado a criar seus próprios aplicativos de comunicação, utilizando criptografia forte

Põe-se todos os usuários em risco

- Não é uma questão de "**se**" atores maliciosos terão acesso aos sistemas que guardam as chaves ou o texto em claro
- Mas sim de o que fazer "**quando**" eles tiverem acesso

A sociedade perde a confiança na tecnologia

- Inibe-se a inovação
- Reduz-se a qualidade de vida

Desafios para o Futuro

Qualificação profissional

- redes, administração de sistemas, segurança, **desenvolvimento de *software* seguro**

Certificação de dispositivos não faz mais sentido

- não há como certificar *software* (*firmware* é *software*)

Vulnerabilidades sempre vão existir

- o importante é tratá-las de forma rápida

Precisamos discutir, em nível global, a definição de requisitos de maturidade em segurança para fabricantes

- possuir ciclo claro de atualização de *software/firmware*
- possuir um PSIRT (*Product Security Incident Response Team*) ou ao menos um contato claro para tratar problemas de segurança no produto
  - referências:
    - *FIRST PSIRT Services Framework* https://first.org/education/Draft_FIRST_PSIRT_Service_Framework_v1.0
    - *The Building Security In Maturity Model* https://www.bsimm.com/

Segurança é inerentemente multissetorial: **Cooperação para um ecossistema saudável**

Nenhum grupo ou estrutura única conseguirá fazer sozinha a segurança ou a resposta a incidentes - todos tem um papel

- universidades
  - precisam incluir questões de segurança em todas as disciplinas
  - desenvolvimento seguro precisa ser prioridade desde o início
- desenvolvedores / empresas
  - precisam pensar em segurança desde as etapas iniciais de desenvolvimento
- gestores
  - precisam considerar segurança como um investimento e alocar recursos adequados
- administradores de redes e sistemas e profissionais de segurança
  - não emanar “sujeira” de suas redes
  - adotar boas práticas
- usuários
  - entender os riscos e seguir as dicas de segurança
  - manter seus dispositivos atualizados e tratar infecções

“A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de

medidas técnicas compatíveis com os padrões internacionais e

estímulo ao uso das boas práticas.”

– Princípio 8: Funcionalidade, segurança e estabilidade
Princípios para a Governança e Uso da Internet, CGI.br

Obrigada

www.cert.br

cristine@cert.br

@certbr

15 de novembro de 2017

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br