nic.br cgi.br | cert.br

20º Fórum de Certificação para Produtos de Telecomunicações

30 de novembro de 2016
Campinas, SP

Problemas de Segurança e Incidentes com CPEs e Outros Dispositivos

Cristine Hoepers
cristine@cert.br

cert.br nic.br cgi.br

Incidentes Acompanhados pelo CERT.br

cert.br nic.br cgi.br

Ataques Envolvendo CPEs

Grande base vulnerável

- sem gerência remota
- sem instalação de *patches*
- configurações padrão de fábrica inseguras
  - senhas padrão
  - serviços como Telnet habilitados
  - serviços UDP permitindo abuso para amplificação
    - como SNMP, SSDP, DNS recursivo aberto

Usados para todos os tipos de ataque

- *botnets* para DDoS
- *botnets* para mineração de *bitcoins*
- comprometimento para alteração de DNS

Ataques Envolvendo CPEs para Alteração de DNS

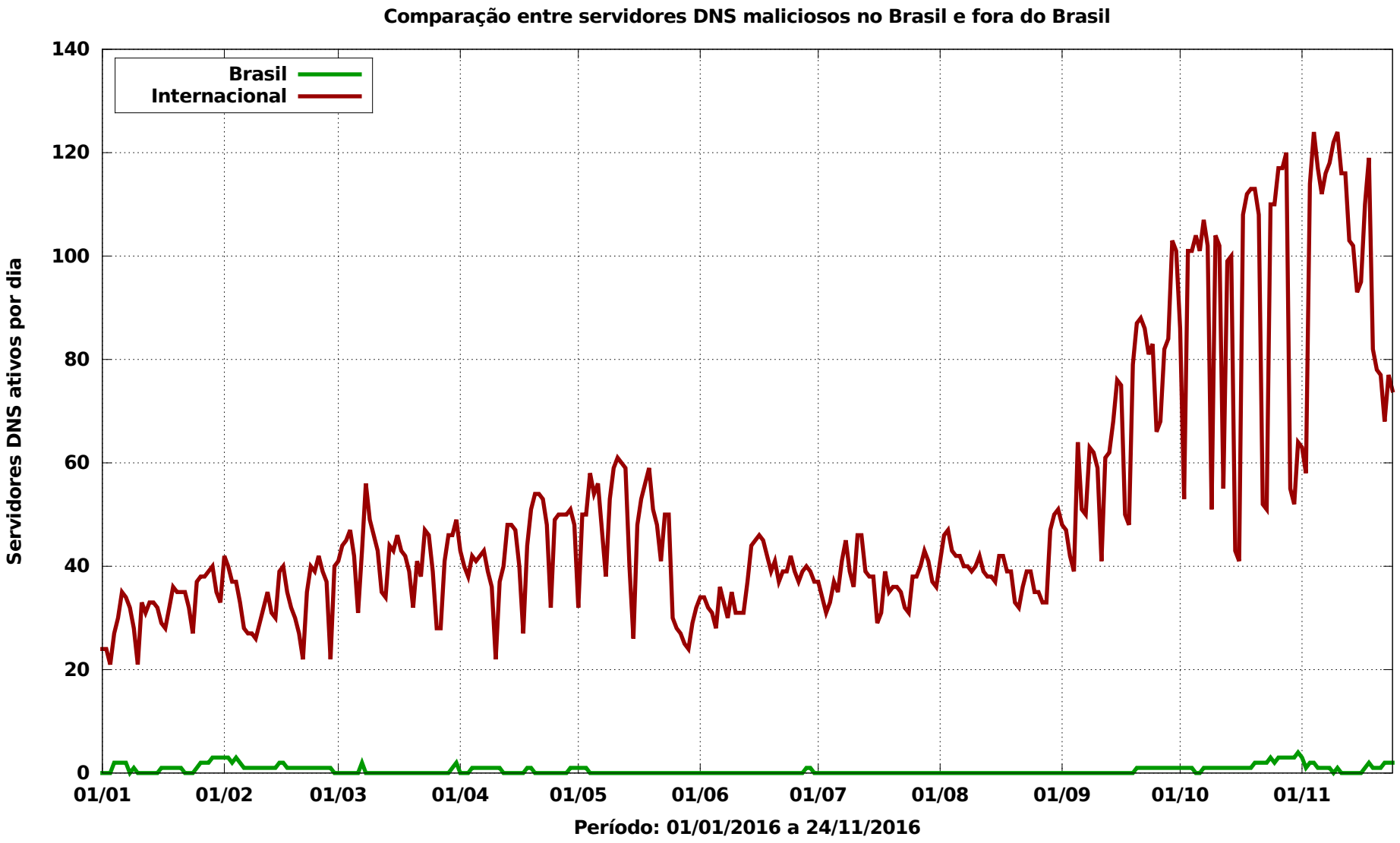
Comprometidos

- via força bruta de senhas (geralmente via telnet)
  - via rede ou via *malware* nos computadores das vítimas
- explorando vulnerabilidades
- via ataques CSRF, através de *iFrames* com *JavaScripts* maliciosos
  - Colocados em *sites* legítimos comprometidos pelos fraudadores

Objetivos dos ataques

- alterar a configuração de DNS para que consultem servidores sob controle dos atacantes
- servidores DNS maliciosos hospedados em serviços de *hosting*/*cloud*
  - casos com mais de 30 domínios de redes sociais, serviços de *e-mail*, buscadores, comércio eletrônico, cartões, bancos

Servidores DNS Maliciosos Ativos por Dia



Botnets de CPEs e Dispositivos IoT

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

***Malware* se propaga geralmente via Telnet**

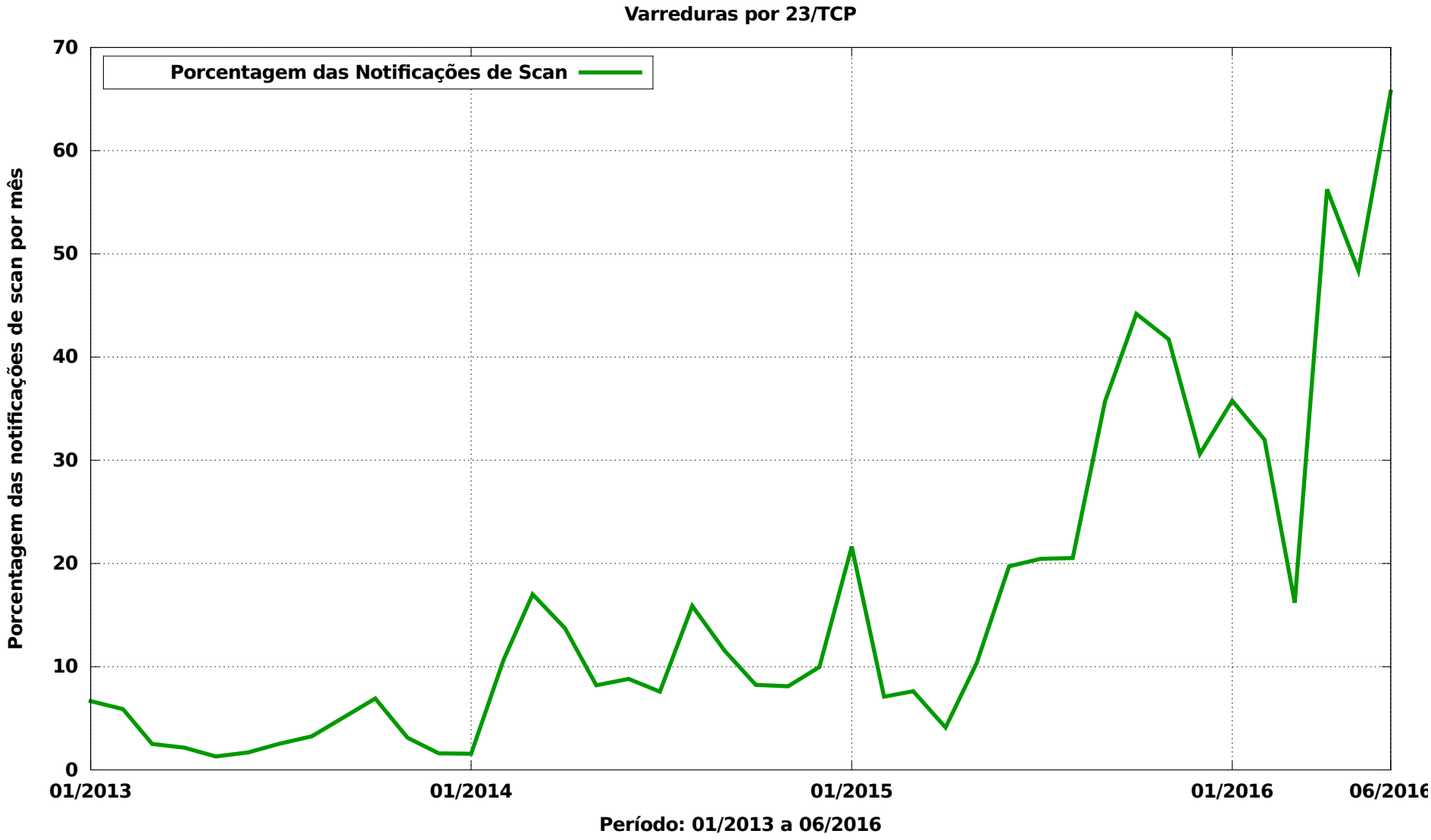
Explora Senhas Fracas ou Padrão

- muitas vezes são "*backdoors*" dos fabricantes

Foco em dispositivos com versões "enxutas" de Linux

- para sistemas embarcados
- arquiteturas ARM, MIPS, PowerPC, etc

Notificações ao CERT.br:
Scans por 23/TCP – 2013 a jun/2016



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

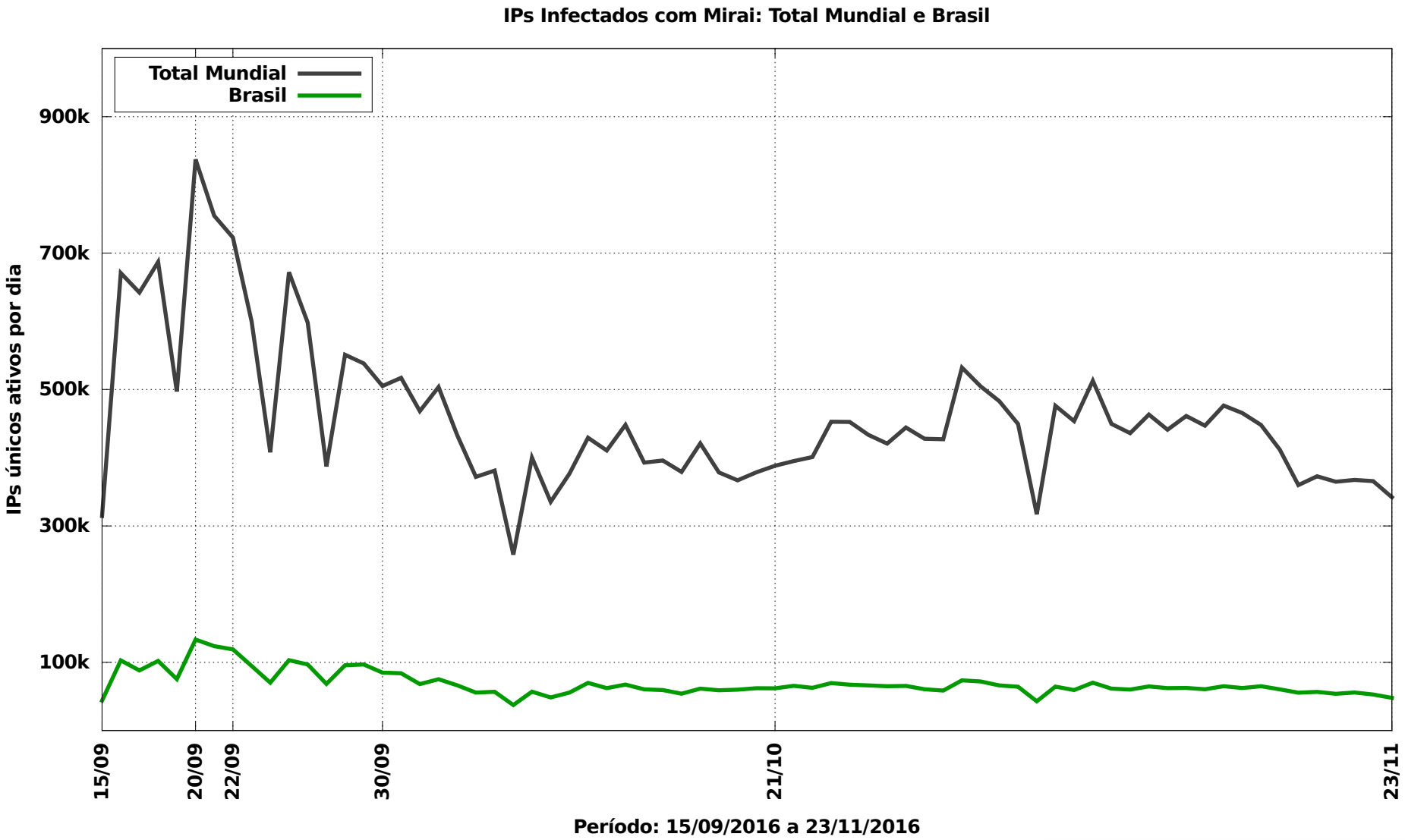
The distributed denial of service (DDoS) attack was aimed at the **website** of industry expert Brian Krebs.

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

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



Novas Vulnerabilidades nos Últimos 6 meses

cert.br nic.br cgi.br

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.

http://www.kb.cert.org/vuls/id/778696

Vulnerability Note VU#970379

Green Packet DX-350 contains insecure default credentials

Original Release date: 20 Oct 2016 | Last revised: 20 Oct 2016

Print Tweet Send Share

Overview

Green Packet DX-350 uses default credentials

Description

CWE-255: Credentials Management - CVE-2016-6552

Green Packet DX-350 uses non-random default credentials of: root:wimax. A remote network attacker can gain privileged access to a vulnerable device.

Impact

A remote attacker can take complete control of a device using default admin credentials.

Solution

The CERT/CC is currently unaware of a practical solution to this problem.

http://www.kb.cert.org/vuls/id/970379

Vulnerability Note VU#200907

Intellian Satellite TV t-Series and v-Series firmware contains insecure default credentials

Original Release date: 20 Oct 2016 | Last revised: 20 Oct 2016

Print Tweet Send Share

Overview

Intellian Satellite TV antennas t-Series and v-Series, firmware version 1.07, uses default credentials.

Description

CWE-255: Credentials Management - CVE-2016-6551

Intellian Satellite TV antennas t-Series and v-Series, firmware version 1.07, uses non-random default credentials of: ftp/ftp or intellian:12345678. A remote network attacker can gain elevated access to a vulnerable device.

Impact

A remote attacker can take control of a device using default credentials.

Solution

The CERT/CC is currently unaware of a practical solution to this problem.

http://www.kb.cert.org/vuls/id/200907

Vulnerability Note VU#677427

D-Link routers HNAP service contains stack-based buffer overflow

Original Release date: 07 Nov 2016 | Last revised: 10 Nov 2016

Print Tweet Send Share

Overview

D-Link DIR routers contain a stack-based buffer overflow in the HNAP Login action.

Description

CWE-121: Stack-based Buffer Overflow - CVE-2016-6563

Proces
stack.

CVE-2

- [
- [
- DIR-818L(W)

Impact

A remote, unauthenticated attacker may be able to execute arbitrary code with root privileges.

Solution

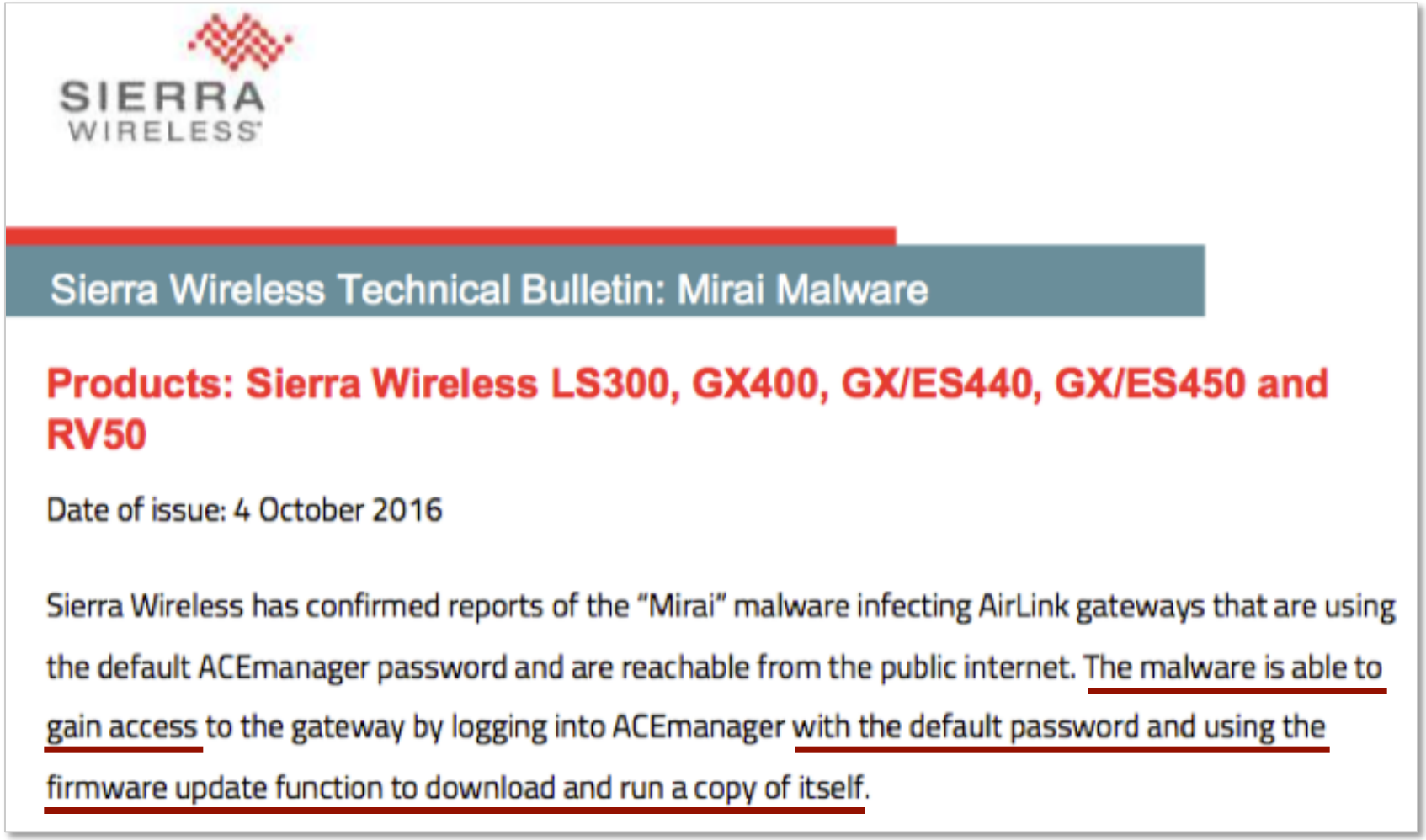
Apply an update

D-Link has released firmware updates to address the vulnerabilities in affected routers. Please see their announcement.

http://www.kb.cert.org/vuls/id/677427

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

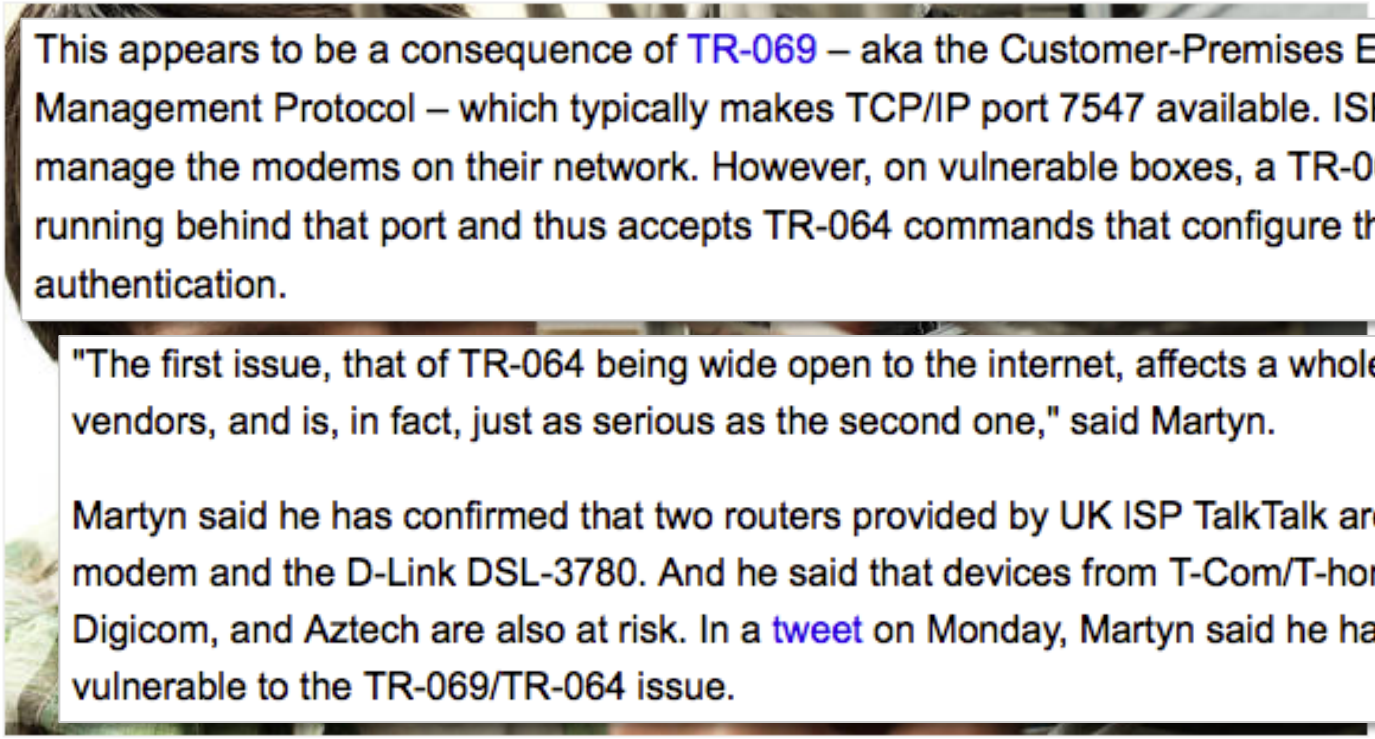
Date of issue: 4 October 2016

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/

'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/

Rede de Honeypots do CERT.br:
Dados de Propagação da Nova Variante de Mirai

Portas TCP que mais sofreram varreduras em 26/11:

23:	6.866.114
7547:	1.637.233
22:	703.706
2323:	560.529
80:	533.487

IPs únicos brasileiros realizando varreduras na porta 7547 e com assinatura da nova variante:

26/11:	323.559
27/11:	573.730
28/11:	245.920

Desafios para Melhorar o Cenário

cert.br nic.br cgi.br

Nos Fabricantes, Velhos Problemas

Preocupação zero com segurança

- "alguém" fará a segurança depois...

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*?

Lições Aprendidas com a Deutsch Telecom

- **Contato pré-estabelecido com o fabricante do CPE**
- **Criação rápida de novo firmware com a correção da vulnerabilidade**
- **Planejamento para gerência e update remotos**
  - maior parte do parque precisa apenas que o CPE seja desligado e ligado novamente para que inicie a busca por um novo *firmware*

Recomendações para Usuários de Equipamentos de Telecomunicações (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

- algum esquema de gerência remota
- como atualizar remotamente

Recomendações para Usuários de Equipamentos de Telecomunicações (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 o caso antigo do CPE da Arris que não permitia desabilitar Telnet

Manter os equipamentos atualizados

Utilizar sempre que possível uma rede de gerência

Obrigada

www.cert.br

cristine@cert.br

@certbr

30 de novembro de 2016

nic.br cgi.br

www.nic.br | www.cgi.br