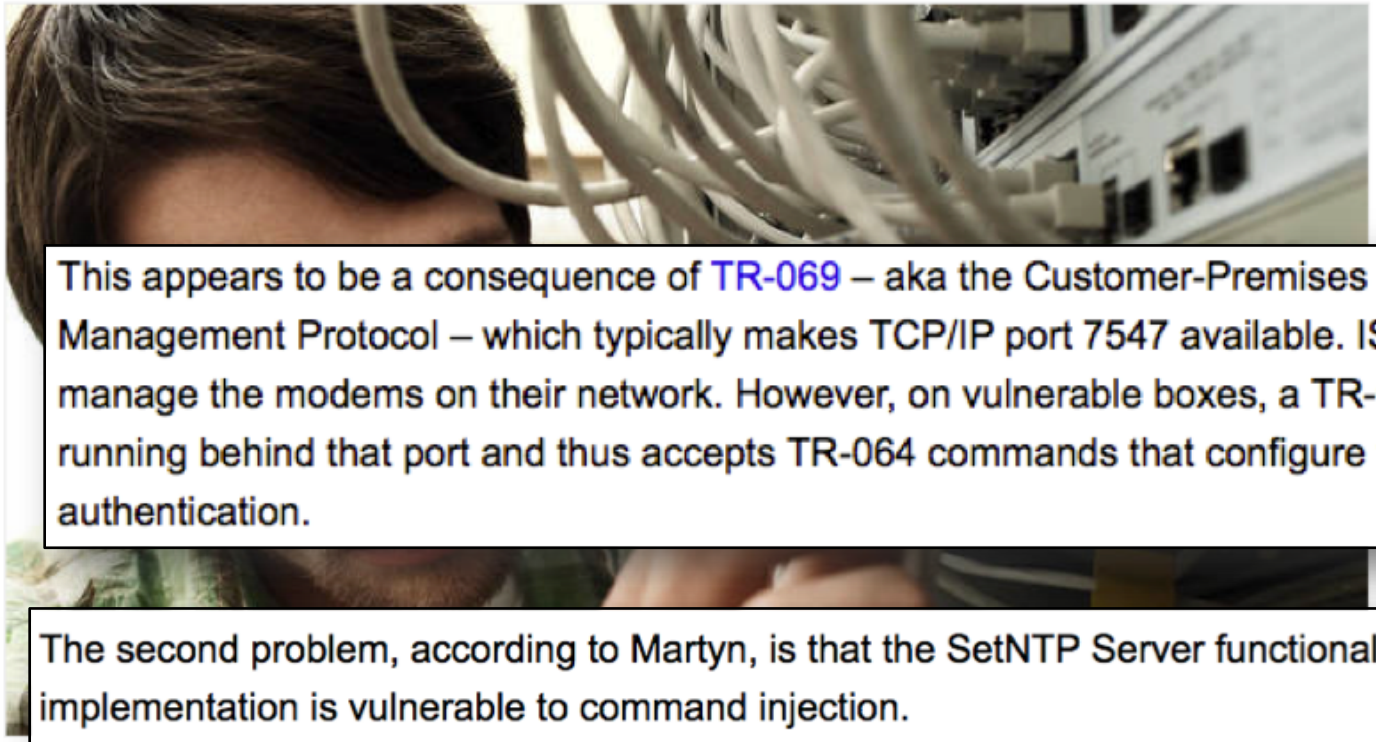
Requisitos mínimos de segurança para aquisição de CPE

GTS 32
14 de dezembro de 2018
São Paulo, SP

Lucimara Desiderá (LAC-AAWG)

'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 second problem, according to Martyn, is that the SetNTP Server functionality in the router's TR-064 implementation is vulnerable to command injection.

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.

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

Por que CPE são alvos?

- Denial of service attacks (DDoS);
- Mineração não autorizada de criptomoedas;
- Propagação de *malware*;
- Envio de *spam*;
- *Phishing*;
- Furto de credenciais.

Impacto

- Impactos operacionais e de negócios
  - Comprometimento da rede do provedor
  - Degradação ou indisponibilidade de serviços
  - Suporte técnico
  - Retrabalho

$$$

(In)Segurança em CPE

- Credencial comum para todos os dispositivos
- Usernames/passwords conhecidas/fáceis de adivinhar (i.e. admin / password)
- Credenciais *hardcoded*
- uso de protocolos e algoritmos obsoletos e inseguros;
- acessos não documentados (*backdoors*)
- falta de mecanismos de atualização seguros e automatizados
- serviços desnecessários e / ou inseguros habilitados por padrão
- serviços que não podem ser desativados;
- gerenciamento remoto inseguro

BCOP Requisitos de Segurança em CPE
Demanda por segurança nativa (*by design* e *by default)*

- Outubro 2017 – LACNIC28 / LACNOG 2017, Montevideo
  - Discussões iniciais e voluntários para desenvolver o documento.
- Abril 2018 – Primeiro draft para comentários
- Maio 2018 – LACNIC29, Panamá (Primeira discussão presencial do draft-01)
- Junho 2018 (draft-02 para comentários /divulgação junto a operadoras e indústria)
- Setembro 2018
  - Lançamento do draft-03 para comentários
  - Discussão presencial no LACNIC30 - LACNOG 2018, Rosario/AR
  - Longo período para comentários (participação de colaboradores externos)
- Dezembro 2018 – lançamento do draft-04
  - “Last Call” na lista BCOP
  - Encaminhado para “Technical Review” pela M3AAWG

BCOP: "*Minimum security requirements for customer premises equipment (CPE) acquisition*"

Table of Contents

https://drive.google.com/file/d/1lv8cFS_SFolGZbigZyGuxtL-qPz5AoQe/view?usp=sharing

Como participar

- BCOP em desenvolvimento
  - *"Minimum security requirements for customer premises equipment (CPE) acquisition"*

    https://docs.google.com/document/d/1Ck3hPVqjQosZuTXcPmFPVKKS6jLylmCtJy5-K0b64j0/edit?usp=sharing

- Lista BCOP bcop@lacnog.org
  - lista aberta do Grupo de Trabalho BCOP do LACNOG, destinada a discussão de melhores práticas operacionais para serviços de redes

    http://www.lacnog.org/wg-bcops/

    https://mail.lacnic.net/mailman/listinfo/bcop

- contato: ldesidera@nog.lat ou lucimara@cert.br