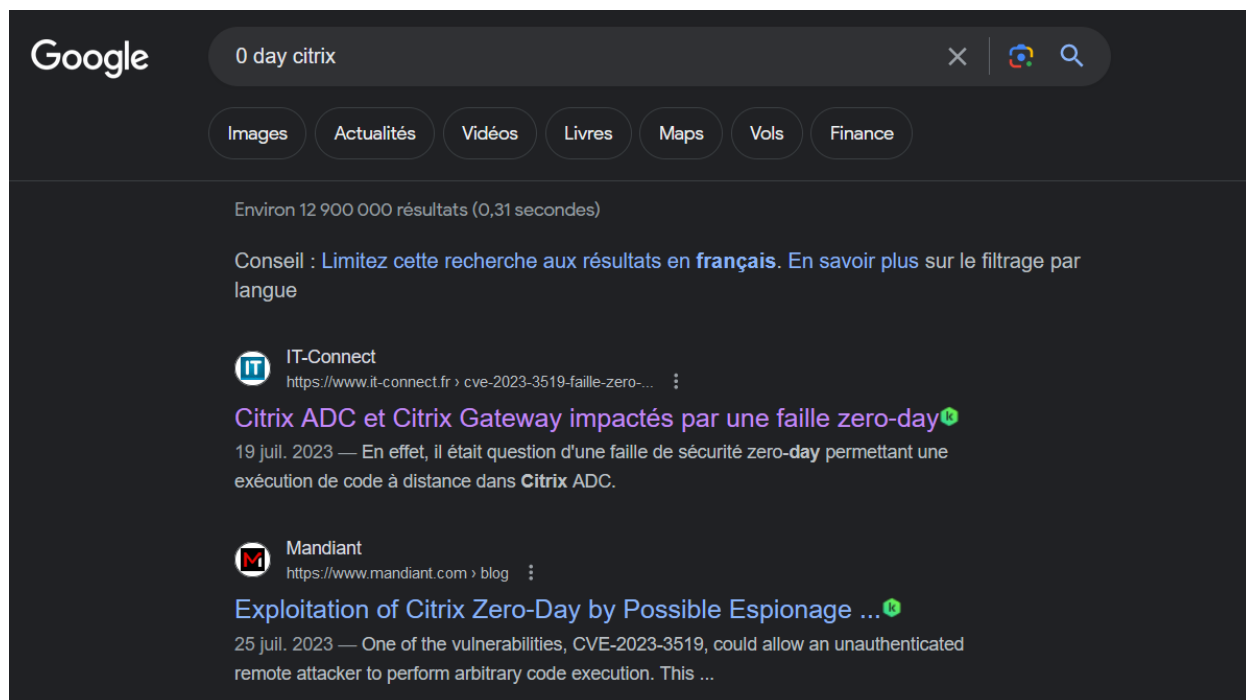


Gateway Vulnerability

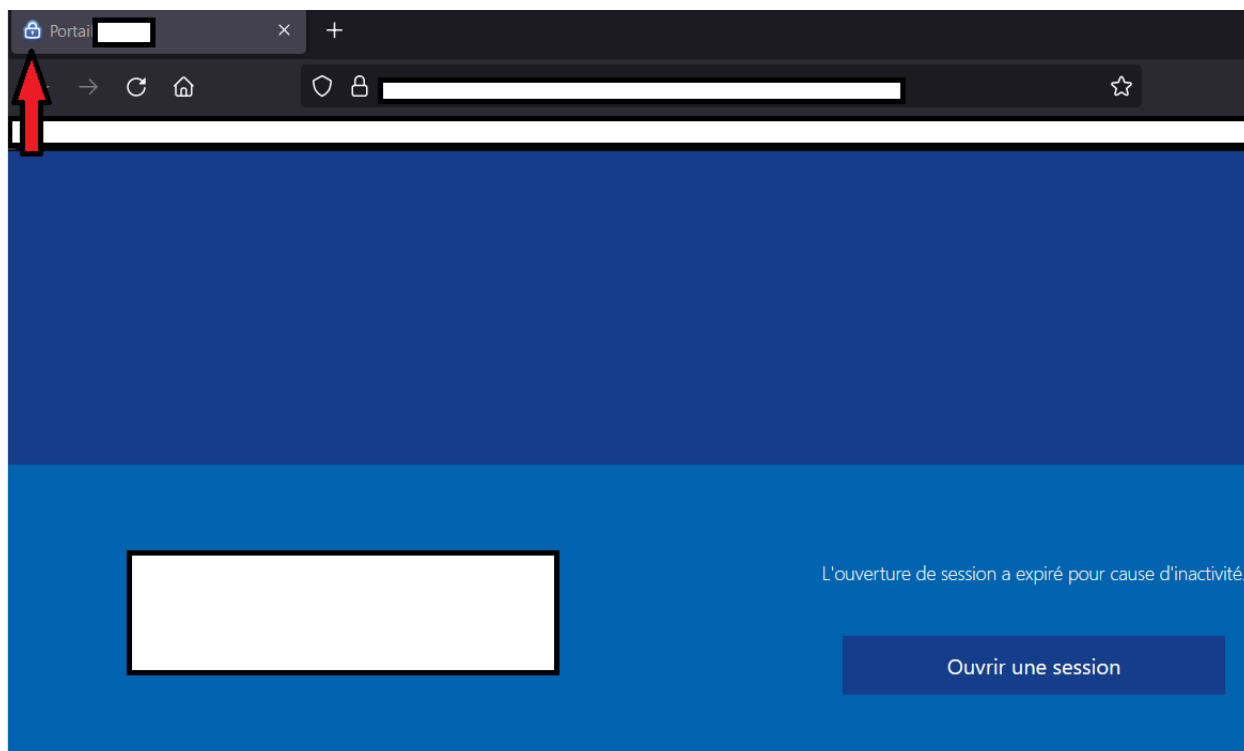


Le premier lien mène vers un article publié par IT-Connent [Citrix 0day article](#) nous donne le numéro de la CVE : CVE-2023-3519

Pour la deuxième partie du chall on cherche les webs technologies utiliser dans la page d'authentification des gateways citrix exposé sur Internet dont dispose l'entreprise Deutsche Gesetzliche Unfallversicherung E.V. (DGUV).

Pour ce faire, on utilise shodan.

Une méthode pour faire ce genre de recherche est de se baser sur le favicon hash de la page d'authentification.



En calculant le hash de ce favicon nous pouvons retrouver toutes les pages d'authent des gateway citrix.

Pour ce faire, on se base sur les travaux suivants : [phor3nsic : favicon_hash_shodan](#) et on modifie un peu son script pour ouvrir un fichier courant.

```
import mmh3
import codecs
import sys

if len(sys.argv) < 2:
    print("[!] Error!")
    print(f"[-] Use: python3 {sys.argv[0]} path/to/image.png")
    print("[i] Get all hosts with the same image hash!")
    sys.exit()

def main():
    try:
        with open(sys.argv[1], 'rb') as image_file:
            image_content = image_file.read()
    except FileNotFoundError:
        print("[!] Error: File not found.")
        sys.exit()
    favicon = codecs.encode(image_content, "base64")
    hash_image = mmh3.hash(favicon)

    print("[!] Image hash: " + str(hash_image))
    print("[*] View Results:\n> https://www.shodan.io/search?query=http.favicon.hash%3A" + str(hash_image))
```

```
if __name__ == '__main__':  
    main()
```

```
$ python3 favicon_hash_shodan/favicon_img.py citrix_favicon.ico  
[!] Image hash: -1292923998  
[*] View Results:  
> https://www.shodan.io/search?query=http.favicon.hash%3A-1292923998
```

On peut ensuite faire une recherche shodan avec les filtres suivant :
`http.favicon.hash:-1292923998 org:"Deutsche Gesetzliche Unfallversicherung E.V. (DGUV)"`

SHODAN Explore Downloads Pricing 🔍

TOTAL RESULTS
6

TOP PORTS

Port	Count
443	4
444	1
4444	1

Citrix Gateway

91.224.227.175
bgetem.de
Deutsche Gesetzliche Unfallversicherung e.V. (DGUV)
Germany, Bad Hersfeld

SSL Certificate

Issued By:
- Common Name: SwissSign RSA TLS DV/CA
2021 - 1
- Organization: SwissSign AG

Issued To:
- Common Name: *.bgetem.de

Supported SSL Versions:
TLSv1.2, TLSv1.3

HTTP/1.1 200 OK
Date: Sun, 20 Aug 2023 11:14:57 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Thu, 03 Nov 2022 04:40:46 GMT
ETag: "a732-Sec898f83af80"
Accept-Ranges: bytes
Content-Length: 42802
Feature-Policy: camera 'none'; microphone 'none'; geolocation 'none'
Referer-...

On clique sur n'importe quel résultat :


91.224.227.175

Nausis

☐ Regular View

[Raw Data](#)

KirchheimAsbach

 **General** Information

Hostnames

bgetem.de

Domains

BGETEM.DE

Country

Germany

City

Bad Hersfeld

Organization


Deutsche Gesetzliche Unfallversicherung e.V. (DGUV)


ISP


Deutsche Gesetzliche Unfallversicherung e.V. (DGUV)

ASN


AS56532

 **Web** Technologies

 HAMMER.JS

 JQUERY

JQUERY MIGRATE

 JQUERY UI

SLICK

Flag : NBCTF{CVE-2023-28479:flask_sql_html_css_js_apache-server}