PT LAB

Pentesting of EIA blockchain

Ing. David Malaník, Ph.D.
PT LAB – Penetration Testing Laboratory
Faculty of Applied Informatics
Tomas Bata University in Zlín
E-mail: dmalanik@utb.cz

Penetration testing workflow

Get suitable information

Identification of weak points or vulnerabilities

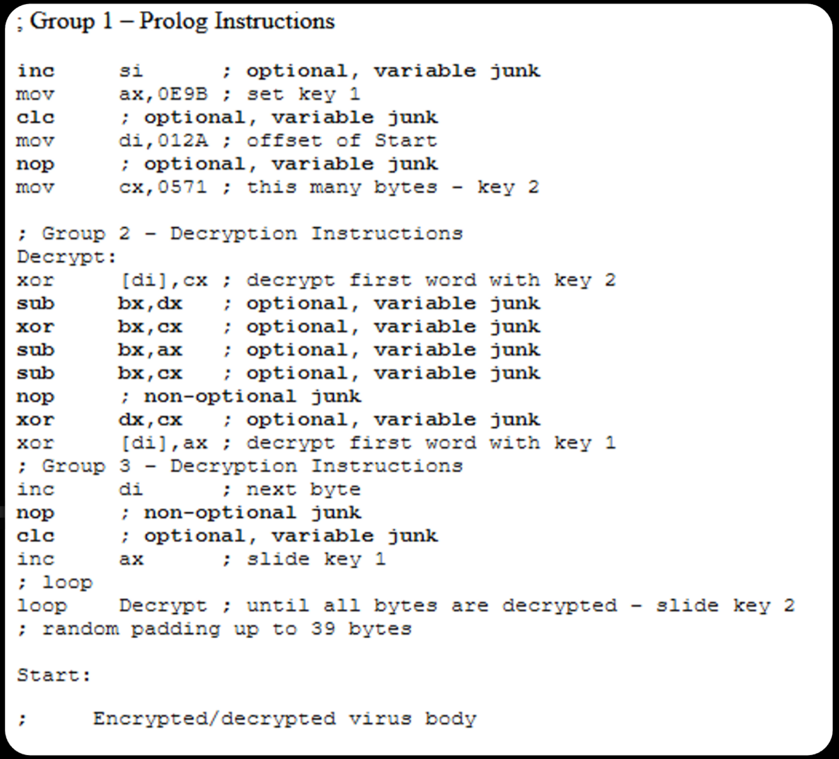
Searching for exploits (create exploit)

Verify exploit functions

Pentest types

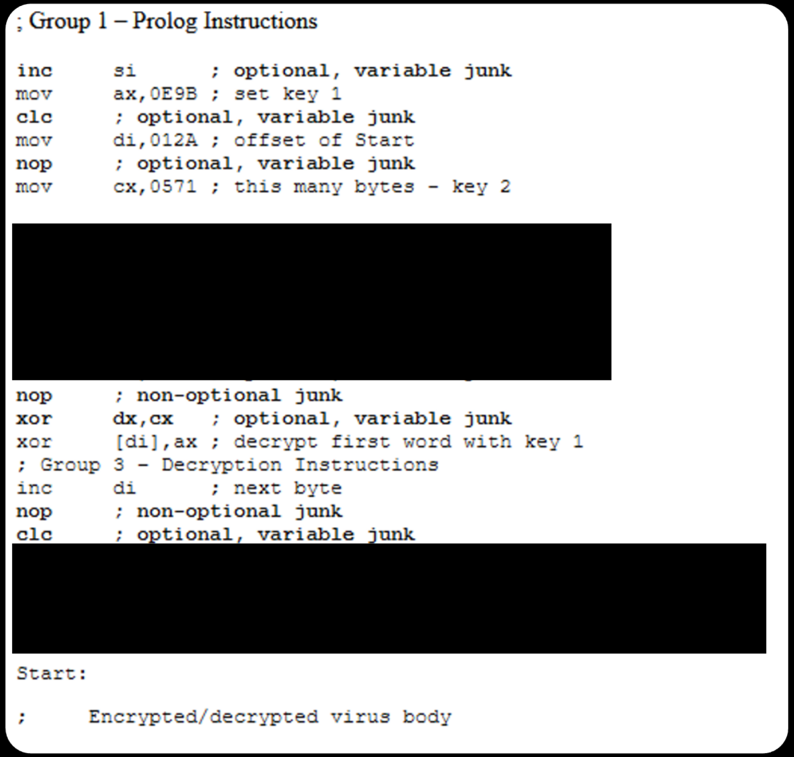
Black box

White box



```
; Group 1 – Prolog Instructions

inc      si       ; optional, variable junk
mov      ax,0E9B  ; set key 1
clc      ; optional, variable junk
mov      di,012A  ; offset of Start
nop      ; optional, variable junk
mov      cx,0571  ; this many bytes - key 2

; Group 2 - Decryption Instructions
Decrypt:
xor      [di],cx  ; decrypt first word with key 2
sub      bx,dx    ; optional, variable junk
xor      bx,cx    ; optional, variable junk
sub      bx,ax    ; optional, variable junk
sub      bx,cx    ; optional, variable junk
nop      ; non-optional junk
xor      dx,cx    ; optional, variable junk
xor      [di],ax  ; decrypt first word with key 1
; Group 3 - Decryption Instructions
inc      di       ; next byte
nop      ; non-optional junk
clc      ; optional, variable junk
inc      ax       ; slide key 1
; loop
loop     Decrypt ; until all bytes are decrypted - slide key 2
; random padding up to 39 bytes

Start:

;     Encrypted/decrypted virus body
```

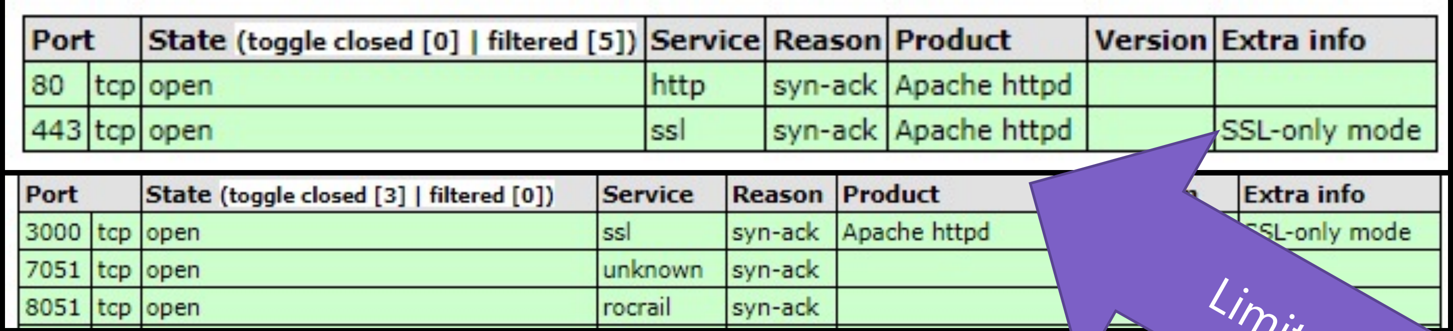
Gray box



```
; Group 1 – Prolog Instructions

inc      si       ; optional, variable junk
mov      ax,0E9B  ; set key 1
clc      ; optional, variable junk
mov      di,012A  ; offset of Start
nop      ; optional, variable junk
mov      cx,0571  ; this many bytes - key 2

[redacted]
nop      ; non-optional junk
xor      dx,cx    ; optional, variable junk
xor      [di],ax  ; decrypt first word with key 1
; Group 3 - Decryption Instructions
inc      di       ; next byte
nop      ; non-optional junk
clc      ; optional, variable junk
[redacted]

Start:

;     Encrypted/decrypted virus body
```

Get right information

- Port scanning
  - */usr/bin/nmap -T4 -sV -sSU -p T1-65535-oA nmapsBC blockchain.***.***.cz*



Port		State (toggle closed [0] | filtered [5])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Apache httpd		
443	tcp	open	ssl	syn-ack	Apache httpd		SSL-only mode

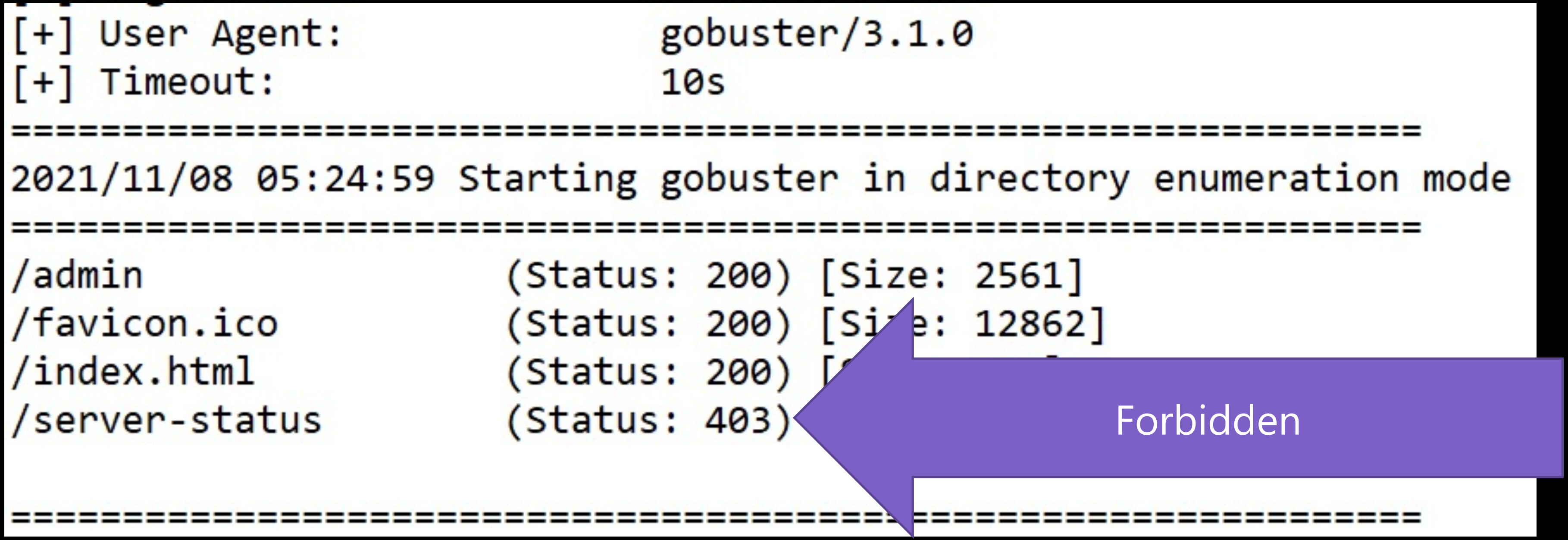
Port		State (toggle closed [3] | filtered [0])	Service	Reason	Product	[illegible]	Extra info
3000	tcp	open	ssl	syn-ack	Apache httpd		SSL-only mode
7051	tcp	open	unknown	syn-ack			
8051	tcp	open	rocrail	syn-ack			

Limited service identification

Limited exploitation possibilities

Get right information

- Web structure enumeration
  - *gobuster dir -u https://blockchain.***.***.cz -w /usr/share/dirb/wordlists/custom.txt*

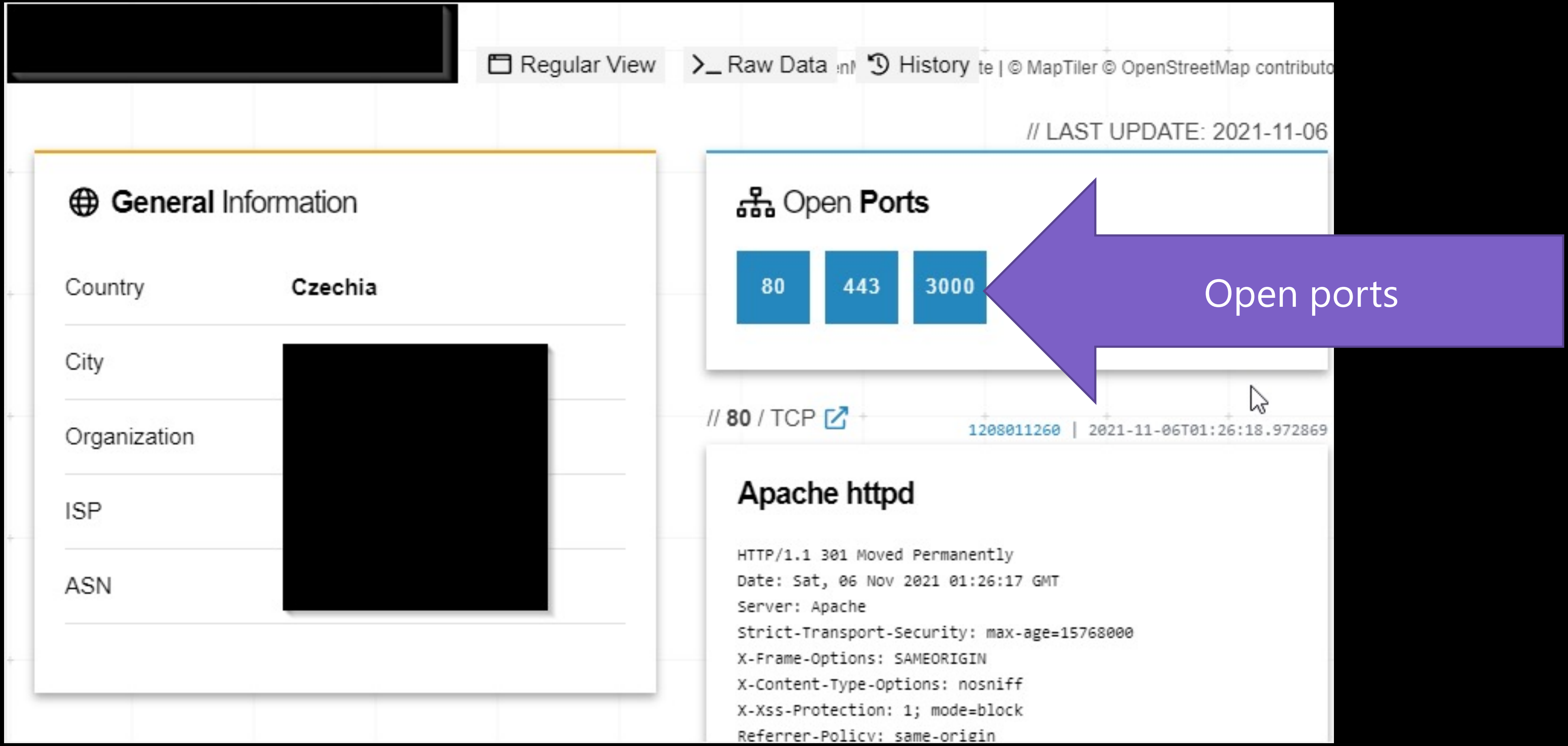


```
[+] User Agent:                gobuster/3.1.0
[+] Timeout:                   10s
===============================================================
2021/11/08 05:24:59 Starting gobuster in directory enumeration mode
===============================================================
/admin                 (Status: 200) [Size: 2561]
/favicon.ico           (Status: 200) [Si e: 12862]
/index.html            (Status: 200) [
/server-status         (Status: 403)


===============================================================
```

Forbidden

Get right information

- Public sources



[redacted]

// LAST UPDATE: 2021-11-06

General Information

Country	Czechia
City	[redacted]
Organization	[redacted]
ISP	[redacted]
ASN	[redacted]

Open Ports

Open ports

// 80 / TCP

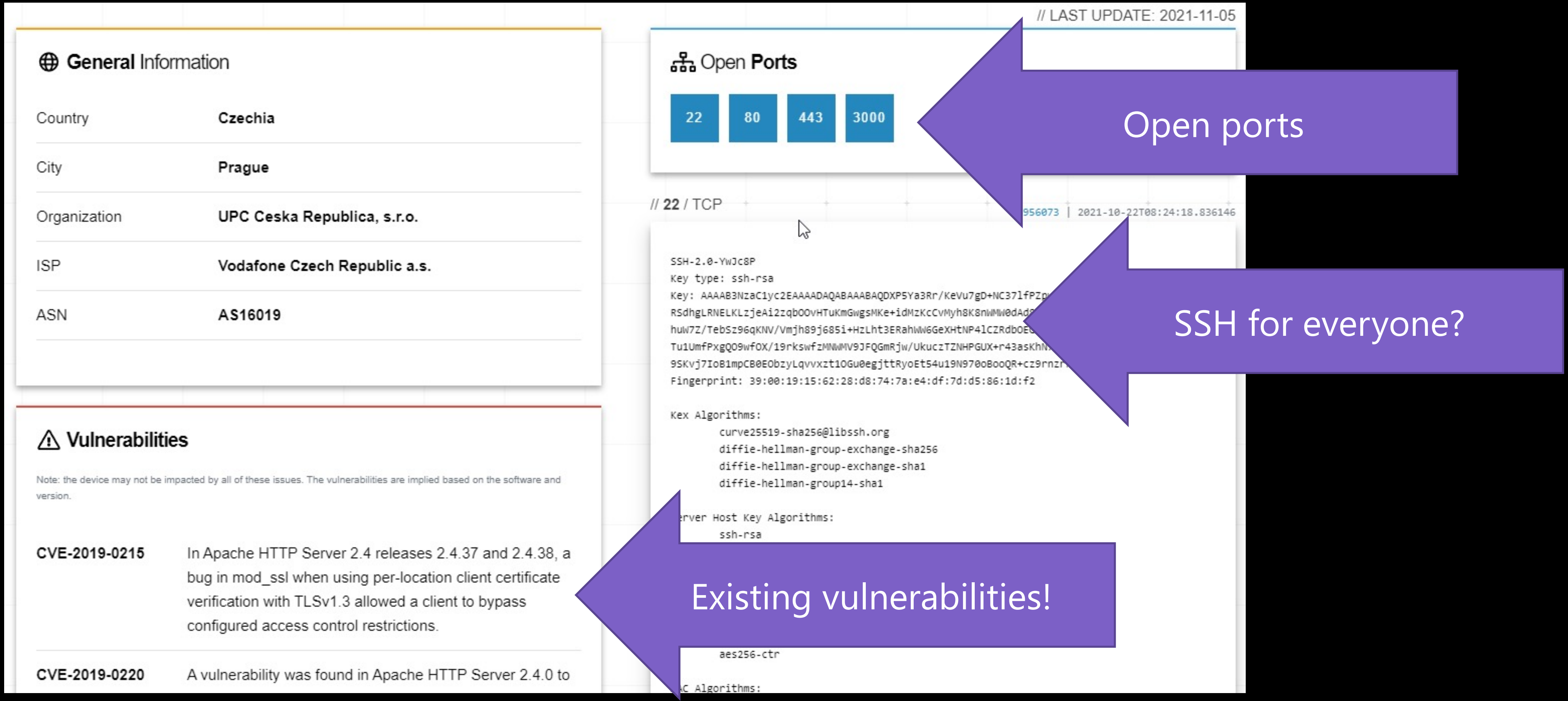
1208011260 | 2021-11-06T01:26:18.972869

Apache httpd

```
HTTP/1.1 301 Moved Permanently
Date: Sat, 06 Nov 2021 01:26:17 GMT
Server: Apache
Strict-Transport-Security: max-age=15768000
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: same-origin
```

Get right information

- Public sources



// LAST UPDATE: 2021-11-05

General Information

Country	**Czechia**
City	**Prague**
Organization	**UPC Ceska Republica, s.r.o.**
ISP	**Vodafone Czech Republic a.s.**
ASN	**AS16019**

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019-0215 In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

CVE-2019-0220 A vulnerability was found in Apache HTTP Server 2.4.0 to

Open **Ports**

22 80 443 3000

// **22** / TCP

956073 | 2021-10-22T08:24:18.836146

```
SSH-2.0-YwJc8P
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDXP5Ya3Rr/KeVu7gD+NC37lfPZp
RSdhgLRNELKLzjeAi2zqbOOvHTuKmGwgsMKe+idMzKcCvMyh8K8nWMW0dAd
huW7Z/TebSz96qKNV/Vmjh89j685i+HzLht3ERahWW6GeXHtNP4lCZRdbOE
Tu1UmfPxgQO9wfOX/19rkswfzMNWMV9JFQGmRjw/UkuczTZNHPGUX+r43asKhN
9SKvj7IoB1mpCB0EObzyLqvvxzt1OGu0egjttRyoEt54u19N970oBooQR+cz9rnzr
Fingerprint: 39:00:19:15:62:28:d8:74:7a:e4:df:7d:d5:86:1d:f2

Kex Algorithms:
        curve25519-sha256@libssh.org
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1

erver Host Key Algorithms:
        ssh-rsa

        aes256-ctr

C Algorithms:
```

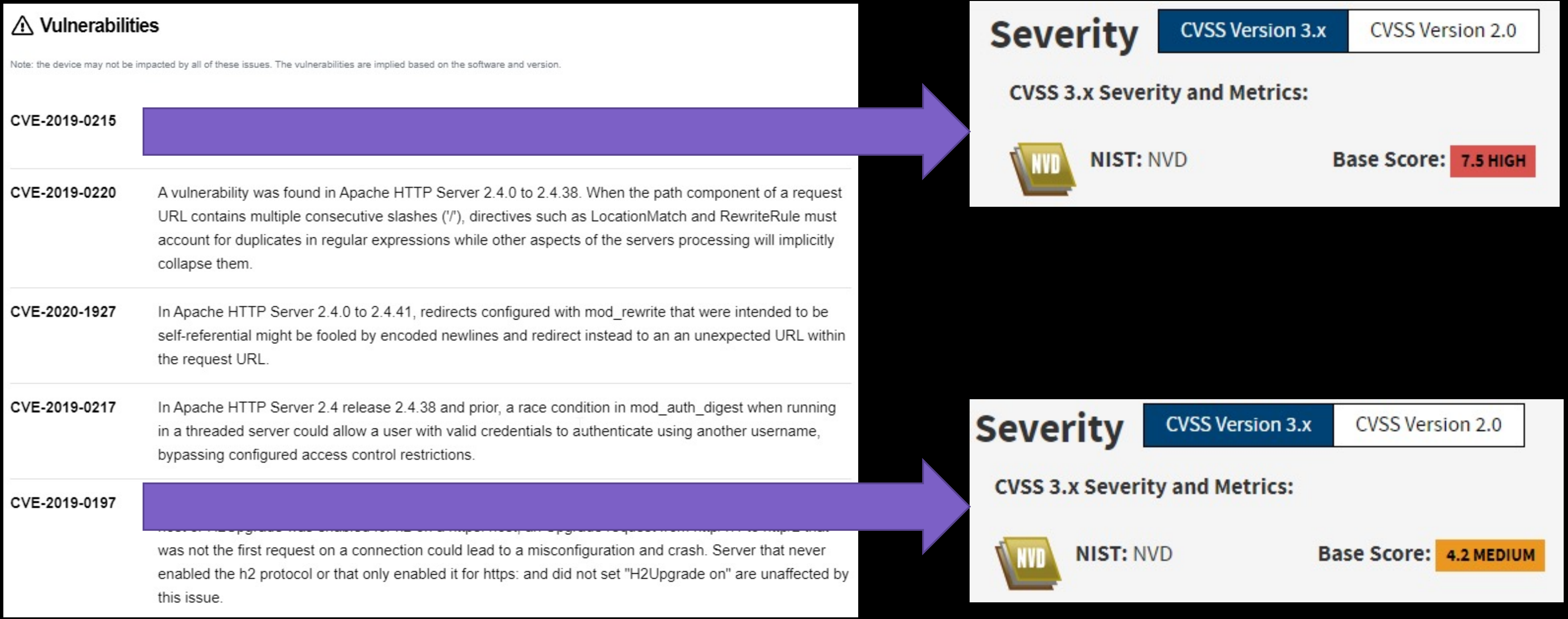
Open ports

SSH for everyone?

Existing vulnerabilities!

Weak points? Vulnerabilities?

- Blockchain „physical“ server



⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019-0215

CVE-2019-0220 A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

CVE-2020-1927 In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

CVE-2019-0217 In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

CVE-2019-0197 was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.5 HIGH

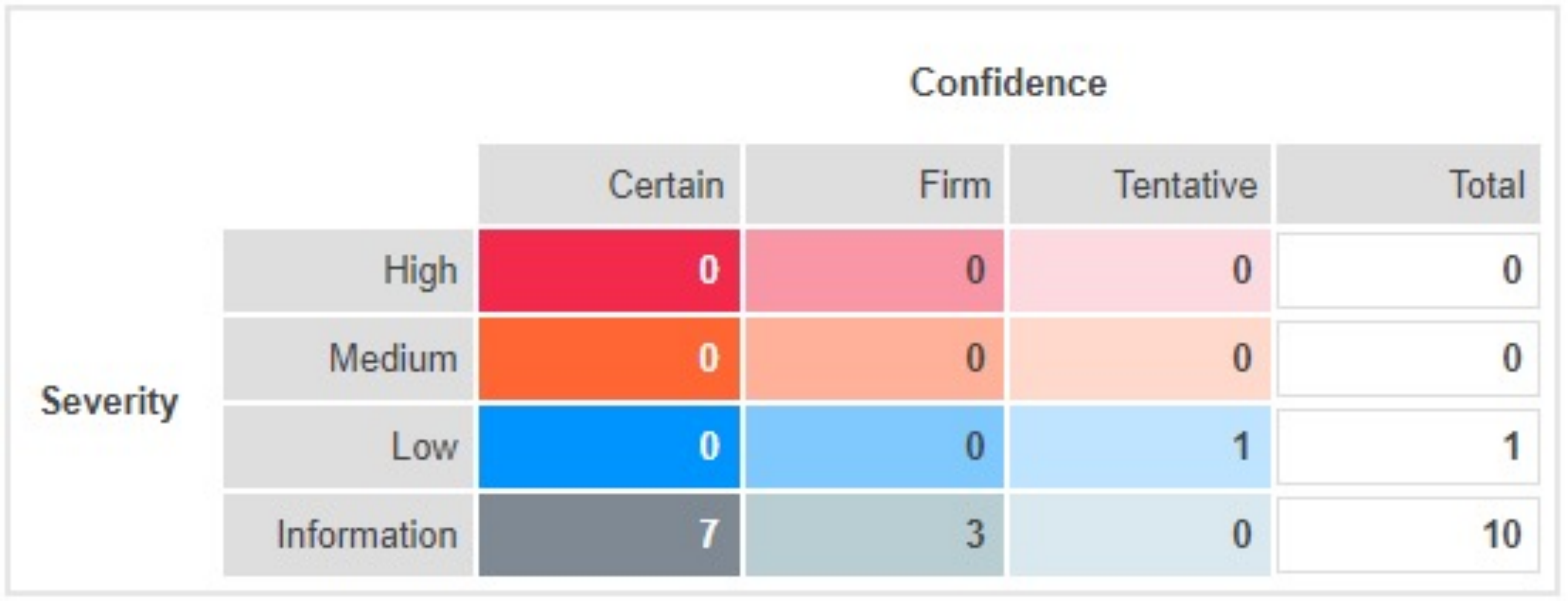
Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 4.2 MEDIUM

Weak points? Vulnerabilities?

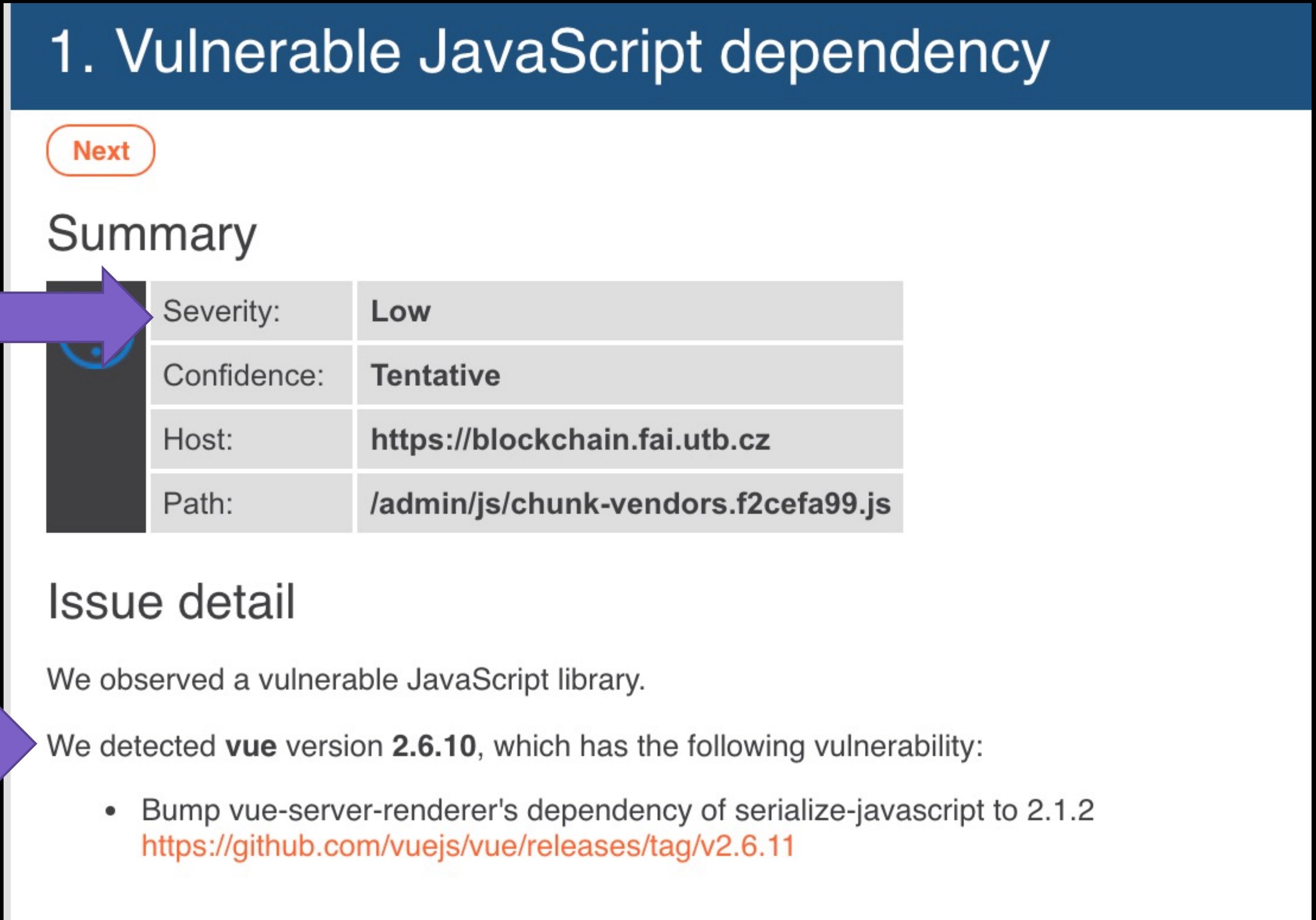
- Blockchain NODE application



		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	0	0
	Medium	0	0	0	0
	Low	0	0	1	1
	Information	7	3	0	10

Weak points? Vulnerabilities?

- Blockchain NODE



1. Vulnerable JavaScript dependency

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://blockchain.fai.utb.cz**
Path:	**/admin/js/chunk-vendors.f2cefa99.js**

Issue detail

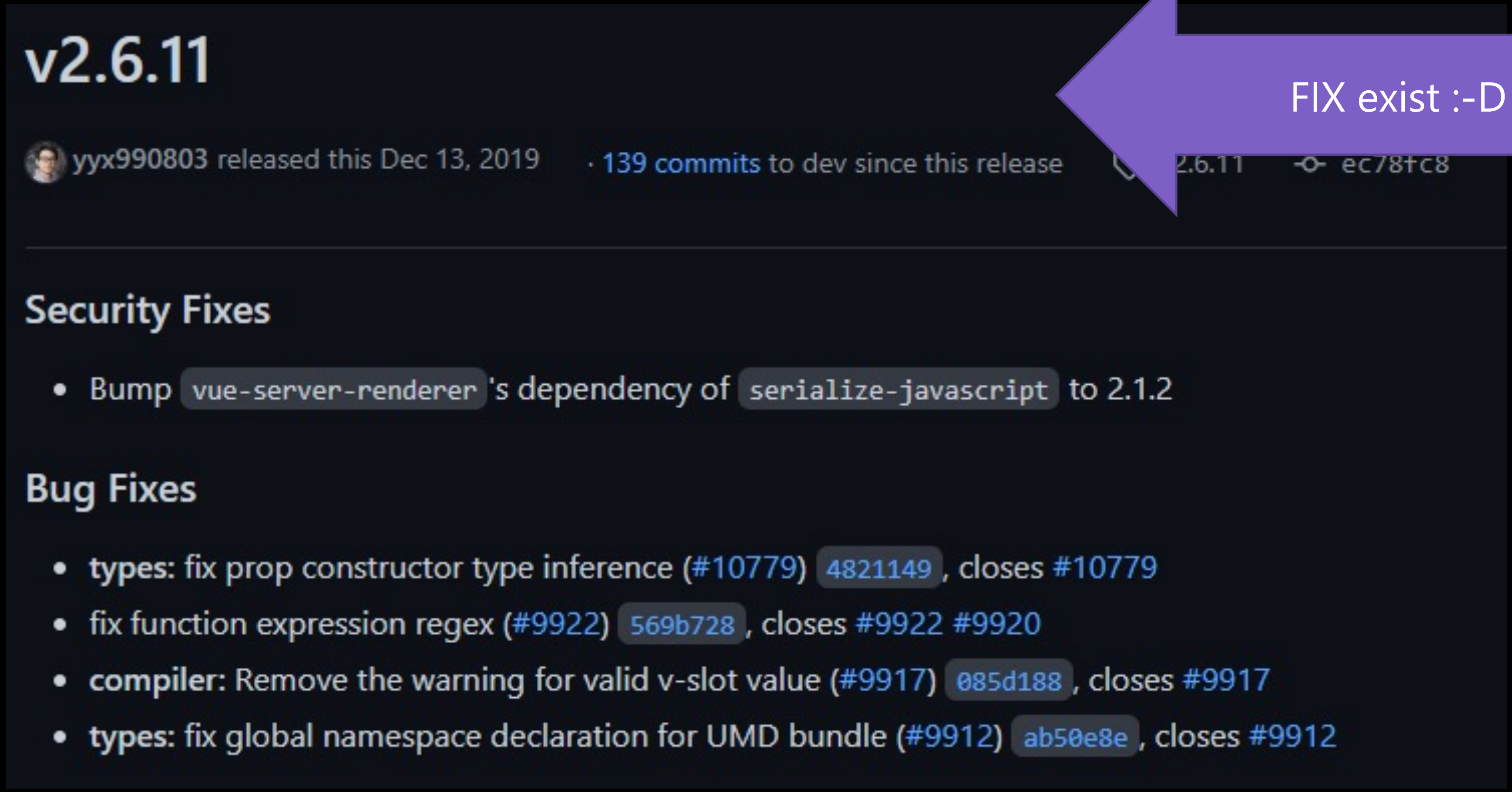
We observed a vulnerable JavaScript library.

We detected **vue** version **2.6.10**, which has the following vulnerability:

- Bump vue-server-renderer's dependency of serialize-javascript to 2.1.2 https://github.com/vuejs/vue/releases/tag/v2.6.11

Weak points? Vulnerabilities?

- Blockchain NODE –vue version 2.6.10



FIX exist :-D

v2.6.11

yyx990803 released this Dec 13, 2019 · 139 commits to dev since this release 2.6.11 ec78fc8

Security Fixes

- Bump `vue-server-renderer`'s dependency of `serialize-javascript` to 2.1.2

Bug Fixes

- **types:** fix prop constructor type inference (#10779) `4821149`, closes #10779
- fix function expression regex (#9922) `569b728`, closes #9922 #9920
- **compiler:** Remove the warning for valid v-slot value (#9917) `085d188`, closes #9917
- **types:** fix global namespace declaration for UMD bundle (#9912) `ab50e8e`, closes #9912

Structure of target + initial attack vectors

Server or VM with Linux OS (mostly) – OS vulnerabilities?

Bunch of docker containers – docker vulnerabilities?

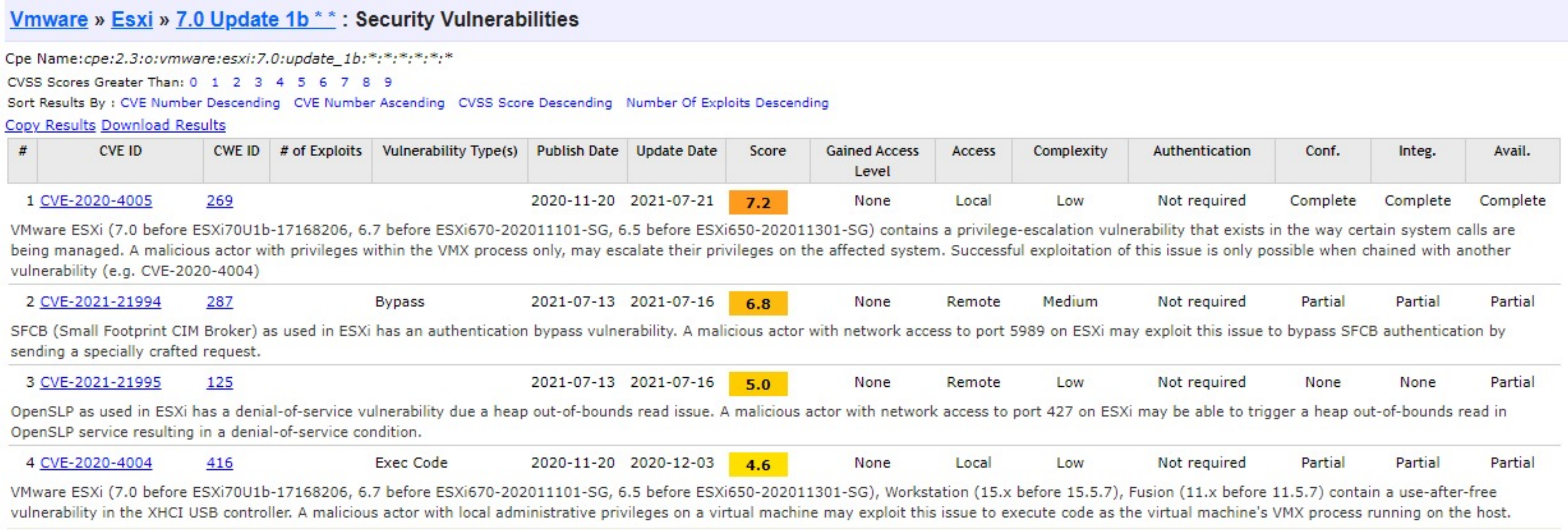
Docker "applications" – vulnerabilities focused to "apps"

Frontends? – web server and app vulnerability

EIA
Blockchain

Server Exploits?

- Attacks focused to server OS/hypervisor
  - OS mostly Linux – various versions – updates needed!



Vmware » Esxi » 7.0 Update 1b * * : Security Vulnerabilities

Cpe Name:*cpe:2.3:o:vmware:esxi:7.0:update_1b:*:*:*:*:*:**

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

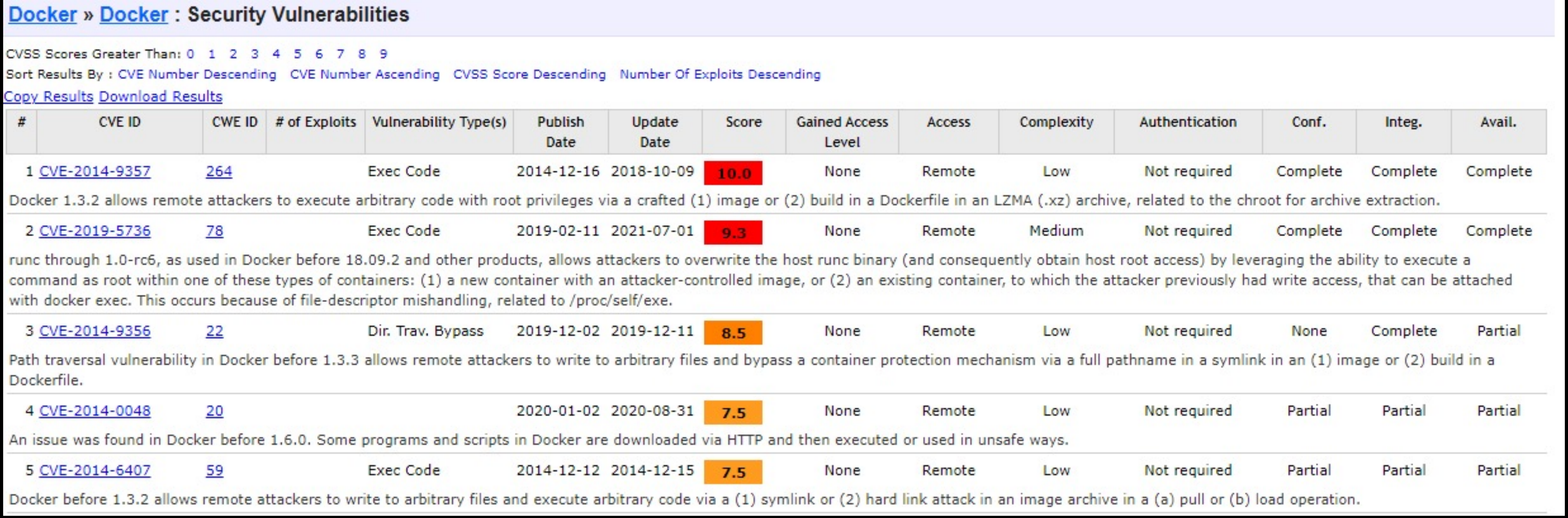
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2020-4005</td><td>269</td><td></td><td></td><td>2020-11-20</td><td>2021-07-21</td><td>7.2</td><td>None</td><td>Local</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG) contains a privilege-escalation vulnerability that exists in the way certain system calls are being managed. A malicious actor with privileges within the VMX process only, may escalate their privileges on the affected system. Successful exploitation of this issue is only possible when chained with another vulnerability (e.g. CVE-2020-4004)</td></tr>
<tr><td>2</td><td>CVE-2021-21994</td><td>287</td><td></td><td>Bypass</td><td>2021-07-13</td><td>2021-07-16</td><td>6.8</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">SFCB (Small Footprint CIM Broker) as used in ESXi has an authentication bypass vulnerability. A malicious actor with network access to port 5989 on ESXi may exploit this issue to bypass SFCB authentication by sending a specially crafted request.</td></tr>
<tr><td>3</td><td>CVE-2021-21995</td><td>125</td><td></td><td></td><td>2021-07-13</td><td>2021-07-16</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">OpenSLP as used in ESXi has a denial-of-service vulnerability due a heap out-of-bounds read issue. A malicious actor with network access to port 427 on ESXi may be able to trigger a heap out-of-bounds read in OpenSLP service resulting in a denial-of-service condition.</td></tr>
<tr><td>4</td><td>CVE-2020-4004</td><td>416</td><td></td><td>Exec Code</td><td>2020-11-20</td><td>2020-12-03</td><td>4.6</td><td>None</td><td>Local</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG), Workstation (15.x before 15.5.7), Fusion (11.x before 11.5.7) contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.</td></tr>
</table>

Docker Exploits?

- Depends of version – update solve many problems



Docker » Docker : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

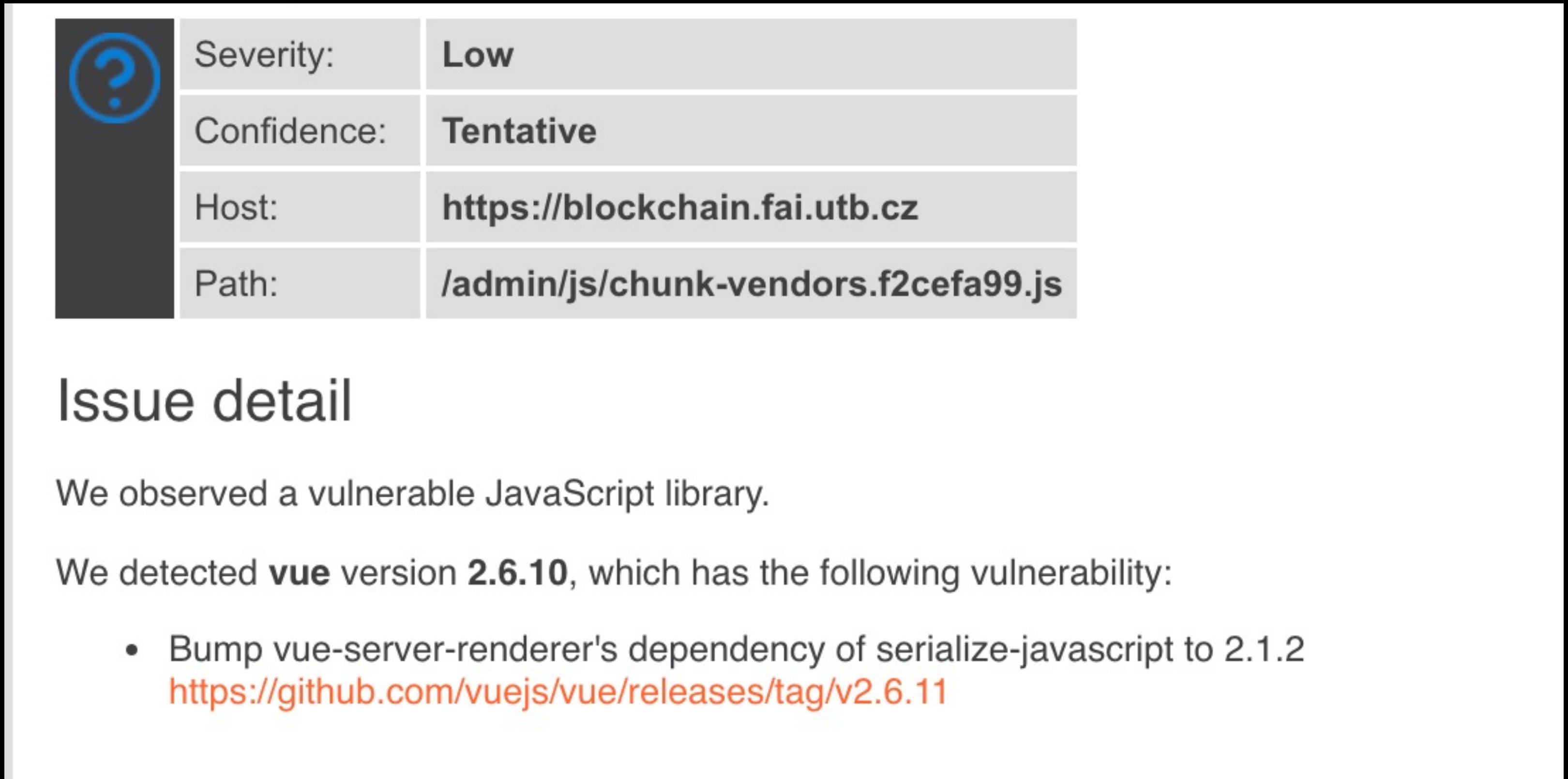
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2014-9357</td><td>264</td><td></td><td>Exec Code</td><td>2014-12-16</td><td>2018-10-09</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Docker 1.3.2 allows remote attackers to execute arbitrary code with root privileges via a crafted (1) image or (2) build in a Dockerfile in an LZMA (.xz) archive, related to the chroot for archive extraction.</td></tr>
<tr><td>2</td><td>CVE-2019-5736</td><td>78</td><td></td><td>Exec Code</td><td>2019-02-11</td><td>2021-07-01</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe.</td></tr>
<tr><td>3</td><td>CVE-2014-9356</td><td>22</td><td></td><td>Dir. Trav. Bypass</td><td>2019-12-02</td><td>2019-12-11</td><td>8.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>Complete</td><td>Partial</td></tr>
<tr><td colspan="15">Path traversal vulnerability in Docker before 1.3.3 allows remote attackers to write to arbitrary files and bypass a container protection mechanism via a full pathname in a symlink in an (1) image or (2) build in a Dockerfile.</td></tr>
<tr><td>4</td><td>CVE-2014-0048</td><td>20</td><td></td><td></td><td>2020-01-02</td><td>2020-08-31</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">An issue was found in Docker before 1.6.0. Some programs and scripts in Docker are downloaded via HTTP and then executed or used in unsafe ways.</td></tr>
<tr><td>5</td><td>CVE-2014-6407</td><td>59</td><td></td><td>Exec Code</td><td>2014-12-12</td><td>2014-12-15</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">Docker before 1.3.2 allows remote attackers to write to arbitrary files and execute arbitrary code via a (1) symlink or (2) hard link attack in an image archive in a (a) pull or (b) load operation.</td></tr>
</table>

Docker apps and frontend Exploits?

- Many updates during whole year
- Hard to detect vulnerable component



Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://blockchain.fai.utb.cz**
Path:	**/admin/js/chunk-vendors.f2cefa99.js**

Issue detail

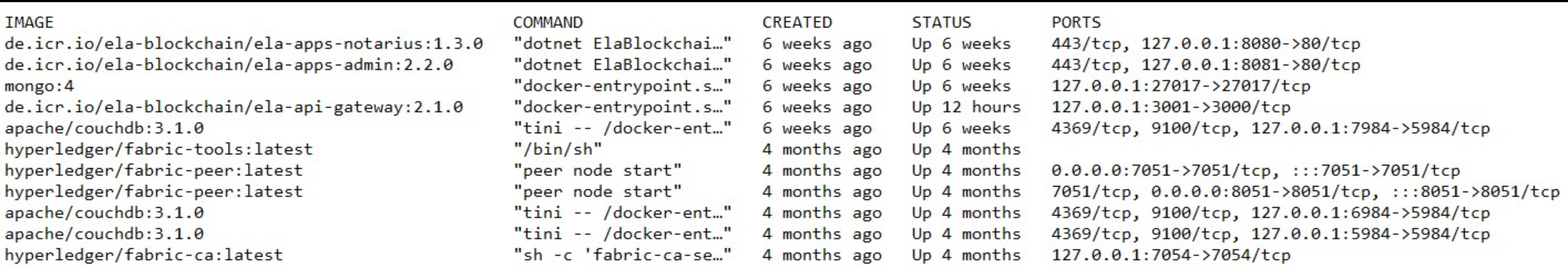
We observed a vulnerable JavaScript library.

We detected **vue** version **2.6.10**, which has the following vulnerability:

- Bump vue-server-renderer's dependency of serialize-javascript to 2.1.2 https://github.com/vuejs/vue/releases/tag/v2.6.11

Additional vulnerabilities – open ports

- Only necessary ports open to public NET
- Minimal attack scope

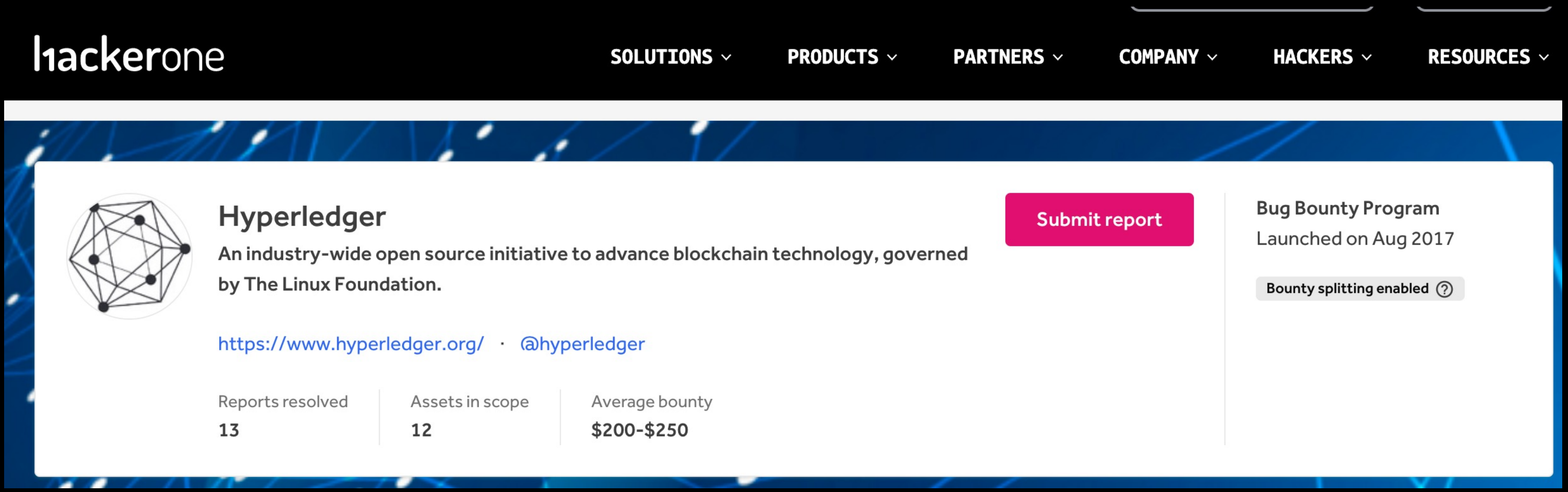


```
IMAGE                                              COMMAND                  CREATED        STATUS        PORTS
de.icr.io/ela-blockchain/ela-apps-notarius:1.3.0   "dotnet ElaBlockchai…"   6 weeks ago    Up 6 weeks    443/tcp, 127.0.0.1:8080->80/tcp
de.icr.io/ela-blockchain/ela-apps-admin:2.2.0      "dotnet ElaBlockchai…"   6 weeks ago    Up 6 weeks    443/tcp, 127.0.0.1:8081->80/tcp
mongo:4                                            "docker-entrypoint.s…"   6 weeks ago    Up 6 weeks    127.0.0.1:27017->27017/tcp
de.icr.io/ela-blockchain/ela-api-gateway:2.1.0     "docker-entrypoint.s…"   6 weeks ago    Up 12 hours   127.0.0.1:3001->3000/tcp
apache/couchdb:3.1.0                               "tini -- /docker-ent…"   6 weeks ago    Up 6 weeks    4369/tcp, 9100/tcp, 127.0.0.1:7984->5984/tcp
hyperledger/fabric-tools:latest                    "/bin/sh"                4 months ago   Up 4 months
hyperledger/fabric-peer:latest                     "peer node start"        4 months ago   Up 4 months   0.0.0.0:7051->7051/tcp, :::7051->7051/tcp
hyperledger/fabric-peer:latest                     "peer node start"        4 months ago   Up 4 months   7051/tcp, 0.0.0.0:8051->8051/tcp, :::8051->8051/tcp
apache/couchdb:3.1.0                               "tini -- /docker-ent…"   4 months ago   Up 4 months   4369/tcp, 9100/tcp, 127.0.0.1:6984->5984/tcp
apache/couchdb:3.1.0                               "tini -- /docker-ent…"   4 months ago   Up 4 months   4369/tcp, 9100/tcp, 127.0.0.1:5984->5984/tcp
hyperledger/fabric-ca:latest                       "sh -c 'fabric-ca-se…"   4 months ago   Up 4 months   127.0.0.1:7054->7054/tcp
```

Security improvements

- Very well professional communication with ELA Blockchain
  - Improvement of blockchain security – vulnerability reporting

- Bug bounty program on Hyperledger platform



Hyperledger

An industry-wide open source initiative to advance blockchain technology, governed by The Linux Foundation.

https://www.hyperledger.org/ · @hyperledger

Reports resolved 13

Assets in scope 12

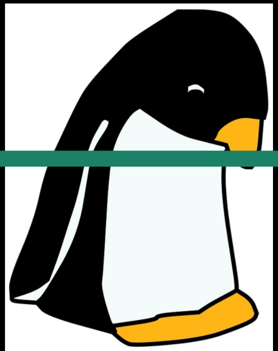
Average bounty $200-$250

Bug Bounty Program

Launched on Aug 2017

Bounty splitting enabled

Conclusion/results



Regular updates!

NODE is secure!

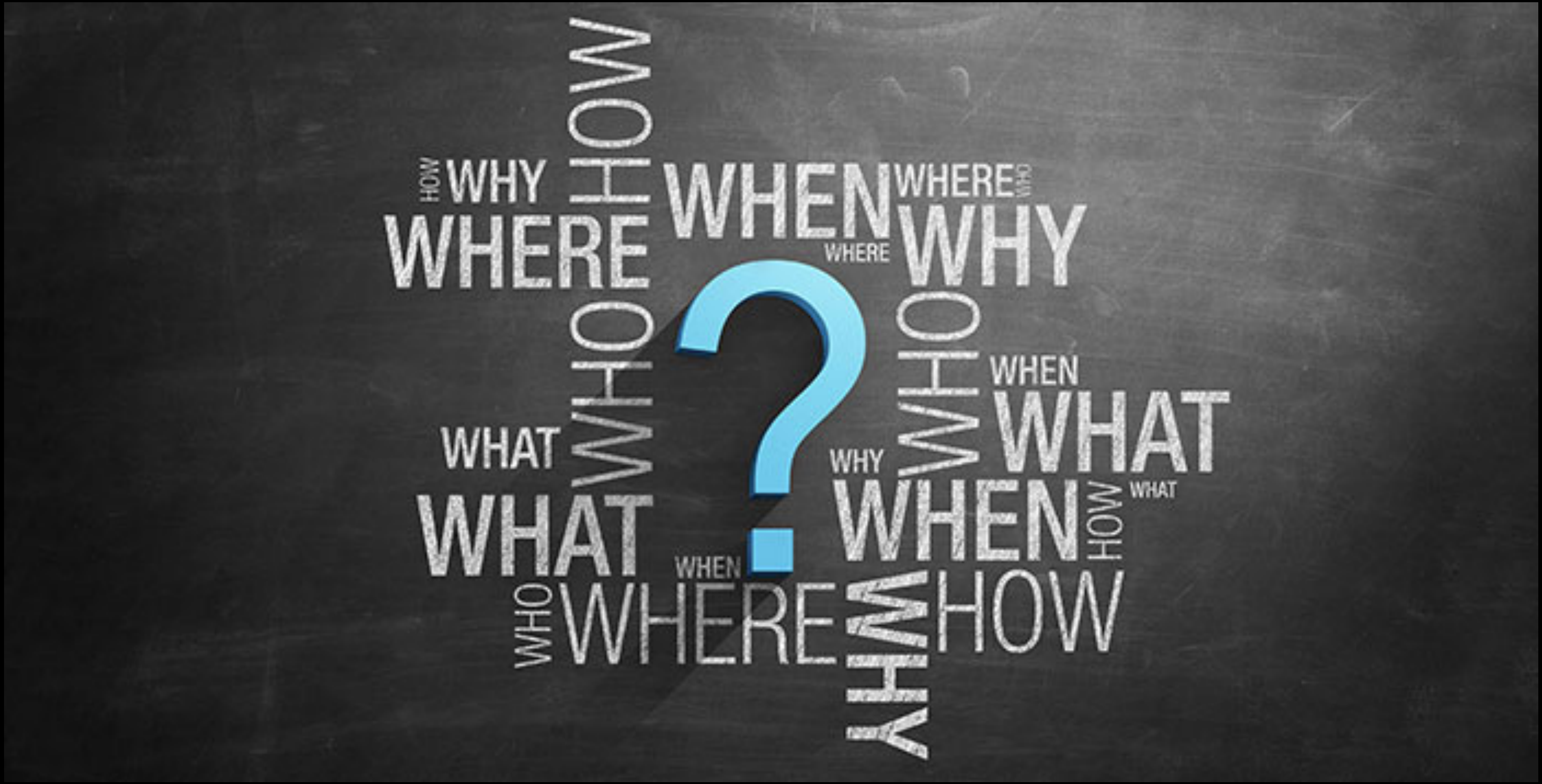
Security improvements!

Superb communication!

Exploitable server OS/hypervisor!

Additional services on server!

Questions>...


HOW
WHY
HOW
WHEN
WHERE
WHO
WHERE
WHERE
WHY
?
WHO
WHO
WHEN
WHAT
WHAT
WHY
WHAT
WHEN
HOW
WHAT
WHEN
WHO
WHERE
WHY
HOW