



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





PT LAB

Pentest types

Black box

White box

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
```

; 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

; 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
```

```
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
```

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	Version	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

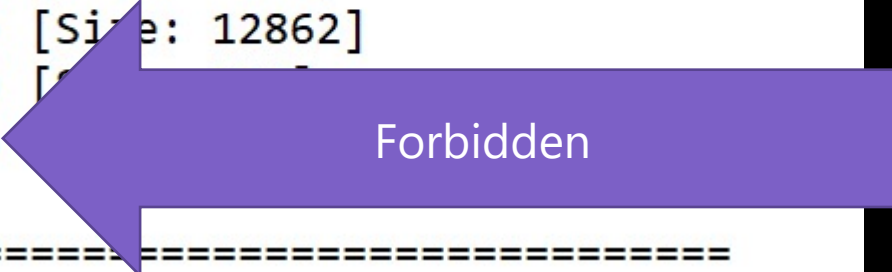
Limited exploitation possibilities



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) [Size: 12862]
/index.html     (Status: 200) [Size: 12862]
/server-status  (Status: 403) [Size: 12862]
=====
```





PT LAB

Get right information

- Public sources

The screenshot displays a web application interface with a dark header and a light main content area. The header includes a search bar, navigation tabs (Regular View, Raw Data, History), and a map attribution. The main content area is divided into two columns. The left column, titled 'General Information', lists fields: Country (Czechia), City, Organization, ISP, and ASN. The right column, titled 'Open Ports', shows three blue boxes with the numbers 80, 443, and 3000. A large purple arrow points from the text 'Open ports' to these boxes. Below the open ports section, there is a section for 'Apache httpd' showing HTTP status and headers. A mouse cursor is visible over the '80 / TCP' link.

Regular View Raw Data History | © MapTiler © OpenStreetMap contributors

// LAST UPDATE: 2021-11-06

General Information

Country **Czechia**

City

Organization

ISP

ASN

Open Ports

80 443 3000

// 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



PT LAB

Get right information

- Public sources

The screenshot displays a public source interface with three main sections:

- General Information:** A table listing details about a device or organization.

General Information	
Country	Czechia
City	Prague
Organization	UPC Ceska Republica, s.r.o.
ISP	Vodafone Czech Republic a.s.
ASN	AS16019
- Open Ports:** A section showing open ports with a last update date of 2021-11-05. The ports listed are 22, 80, 443, and 3000.

// LAST UPDATE: 2021-11-05

Open Ports

22 80 443 3000
- Vulnerabilities:** A section listing known vulnerabilities. It includes a note that the device may not be impacted by all issues and lists two specific CVEs.

⚠ 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

Additional details visible in the screenshot include:

- Open Ports Section:** A sub-section for port 22 / TCP, showing the last update date as 2021-10-22T08:24:18.836146 and a fingerprint of 39:00:19:15:62:28:d8:74:7a:e4:df:7d:d5:86:1d:f2.
- SSH Section:** Details about the SSH configuration, including the key type (ssh-rsa), the key itself, and the Kex Algorithms (curve25519-sha256@libssh.org, diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1).
- Server Host Key Algorithms:** A list of algorithms including ssh-rsa.
- Encryption Algorithms:** A list of algorithms including aes256-ctr.

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	

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

[Next](#)

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

v2.6.11



yyx990803 released this Dec 13, 2019

· 139 commits to dev since this release

2.6.11

ec78fc8

FIX exist :-D

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

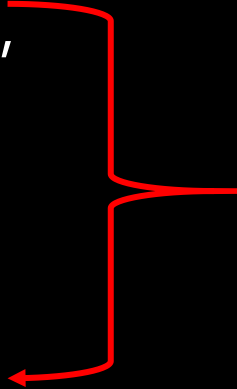
Structure of target + initial attack vectors

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



- 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](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2020-4005	269			2020-11-20	2021-07-21	7.2	None	Local	Low	Not required	Complete	Complete	Complete
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)														
2	CVE-2021-21994	287	Bypass		2021-07-13	2021-07-16	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
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.														
3	CVE-2021-21995	125			2021-07-13	2021-07-16	5.0	None	Remote	Low	Not required	None	None	Partial
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.														
4	CVE-2020-4004	416	Exec Code		2020-11-20	2020-12-03	4.6	None	Local	Low	Not required	Partial	Partial	Partial
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.														



- Depends of version – update solve many problems

- Depends of version – update solve many problems

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](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-9357	264		Exec Code	2014-12-16	2018-10-09	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
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.														
2	CVE-2019-5736	78		Exec Code	2019-02-11	2021-07-01	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
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.														
3	CVE-2014-9356	22		Dir. Trav. Bypass	2019-12-02	2019-12-11	8.5	None	Remote	Low	Not required	None	Complete	Partial
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.														
4	CVE-2014-0048	20			2020-01-02	2020-08-31	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
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.														
5	CVE-2014-6407	59		Exec Code	2014-12-12	2014-12-15	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
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.														

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>



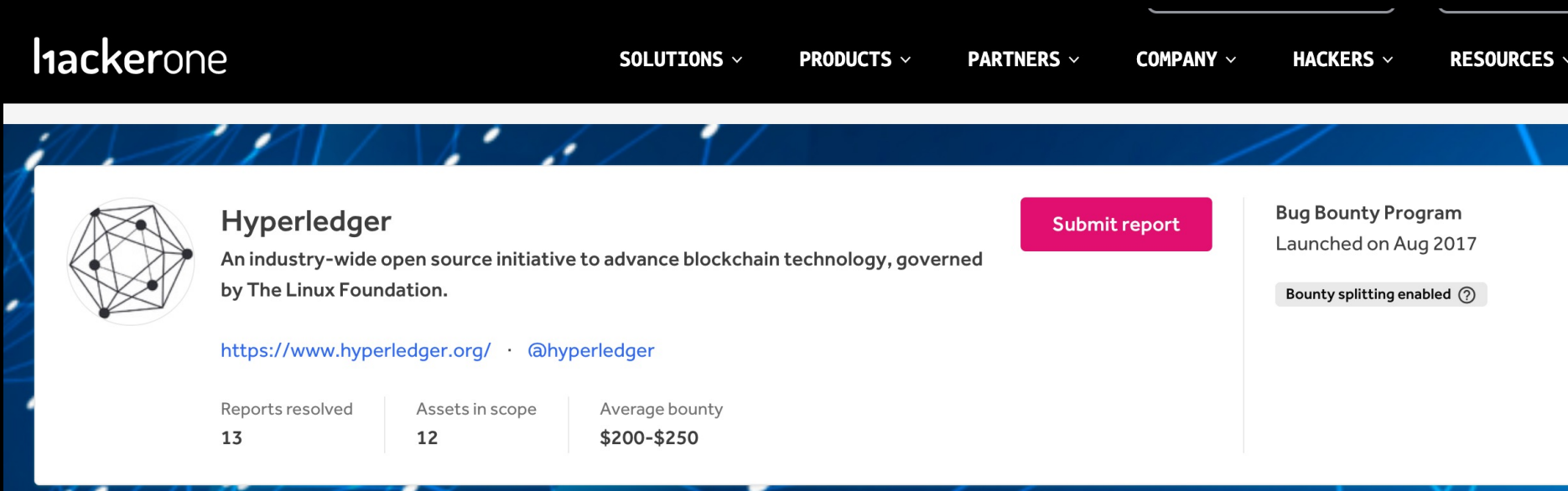
Additional vulnerabilities – open ports

- 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



hackerone SOLUTIONS ▾ PRODUCTS ▾ PARTNERS ▾ COMPANY ▾ HACKERS ▾ RESOURCES ▾



Hyperledger

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

<https://www.hyperledger.org/> · [@hyperledger](https://twitter.com/hyperledger)

Reports resolved	Assets in scope	Average bounty
13	12	\$200-\$250

[Submit report](#)

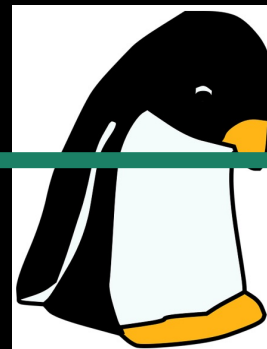
Bug Bounty Program
Launched on Aug 2017

Bounty splitting enabled ⓘ

Conclusion/results

NODE is secure!

Regular updates!



Security improvements!

Superb communication!

Exploitable server OS/hypervisor!

Additional services on server!



PT LAB

Questions > ...

