



IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

Report 03 – Ada Health

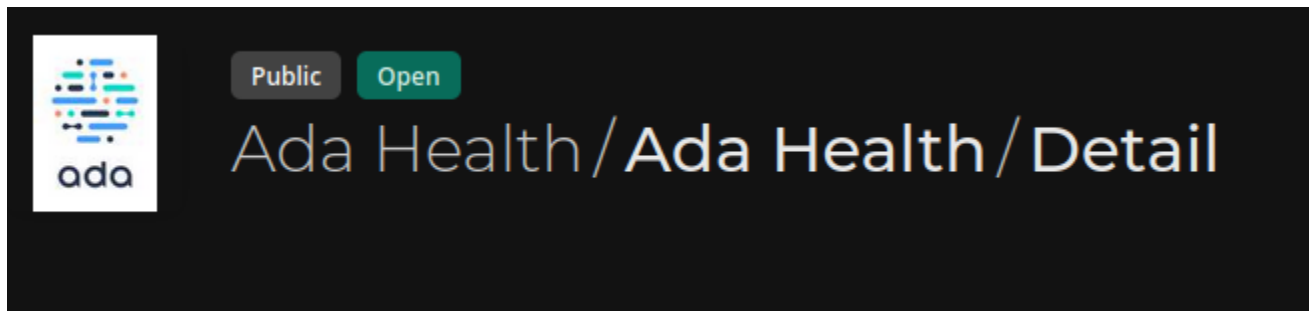
Lecturer in charge – Ms. Chethana Liyanapathirana

IT21826368 – Nanayakkara Y.D.T.D

Contents

1. Ada Health/Ada Health/Detail.....	3
1.1. Overview	3
1.2. Scope	4
1.3. Out of Scope.....	5
1.4. Selected Domain	5
2. Information Gathering	6
2.1. Amass	6
2.2. Knockpy	7
2.3. Dmitry	9
3. Scanning Vulnerability	11
3.1. Scanning ports using Nmap	11
3.2. Scan with rapid scan.	11
4. Vulnerability description.	12
5. Affected components.	12
6. Impact assessment.	13
7. Steps to reproduce.	13
8. Proof of concept (if applicable)	13
9. Proposed mitigation or fix	13
10. Summary	13

1. Ada Health/Ada Health/Detail



1.1.Overview

Description						
Hi, we're Ada. We've been working hard to improve health outcomes since 2016. Built by doctors and scientists and powered by a 10 million-strong user base, our medical AI simplifies healthcare journeys and helps people take care of themselves. We help people understand, manage, and get care for their symptoms with trusted medical expertise in minutes. Our enterprise solutions convert medical knowledge and clinical excellence into better outcomes for our partners.						
Bounties ⓘ						
		Low 0.1 - 3.9	Medium 4.0 - 6.9	High 7.0 - 8.9	Critical 9.0 - 9.4	Exceptional 9.5 - 10.0
Tier 1	€	100	500	1,000	3,000	5,000
Tier 2	€	50	250	750	2,500	4,500
Tier 3	€	50	150	500	1,500	3,500
View changes						

1.2.Scope

In scope

We Are Specifically Looking For

- Accessing any user, customer, or partner sensitive information
- PHI (Protected Health Information) and PII (Personally Identifiable Information)
- Remote Code Execution vulnerabilities are also on our target

OpenAPI Documents

- Assessment BFF Open Api documentation is added as attachment.

Extra Information

- For FHIR and Smart Auth flows, please check the related repositories <https://github.com/adahealth>
- Some endpoints can host OpenApi and GraphQL documentation
- We have stage endpoints without real data corresponding to prod environment. 20 reqs/sec are accepted on stage environments. Reconnaissance techniques can be applied for discovering. Found vulnerabilities for listed assets will be accepted.

SLA Internally

We will validate all submissions within the below timelines, once your submission has been verified by Intigriti. Submissions validated outside of this may be awarded a €25 bonus. This remains at the discretion of Ada Health to award.

Vulnerability Severity	Time to validate
Exceptional	2 Working days
Critical	3 Working days
High	7 Working days
Medium	15 Working days
Low	30 Working days

Working hours = Mon - Fri 9 AM - 5 PM CET

Check Our Fix

We may offer up to €50 bonus to verify a resolved High, Critical, or Exceptional issue. This remains at the discretion of Ada Health to award.

Feedback

Would you like to help us improve our program or have some feedback to share, please send your anonymous feedback here: [Program Feedback Link](#) Please note this form will be checked periodically and **should not** be used for submission or support queries.

1.3.Out of Scope

Out of scope

Out-of-Scope Domains

You will discover the care-navigation ecosystem domains when using the mobile application. Currently, those production environment domains are not in the scope, however their integration environment equivalent domains are in the scope as defined above.

Out-of-Scope Topics

General

- In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited
- Spam, social engineering and physical intrusion
- DoS/DDoS attacks or brute force attacks
- Vulnerabilities that only work on software that no longer receive security updates
- Attacks requiring physical access to a victim's computer/device, man in the middle or compromised user accounts
- Recently discovered zero-day vulnerabilities found in in-scope assets within 14 days after the public release of a patch or mitigation may be reported, but are usually not eligible for a bounty
- Reports that state that software is out of date/vulnerable without a proof-of-concept

1.4.Selected Domain

<https://care-navigation-admin-fe.int.eu.enterprise.ada.com>

Tier 3

URL

Care Navigation Admin Frontend is a visual tool for managing Connect data including:

- Connect Care Option mappings,
- Connect/Assess Feedback service,
- Connect Sign-up service,
- Admin Users,
- Connect Client Configurations

Test credentials will not be provided. Try to find broken access controls on this endpoint.

Hide description ^

In this report I used the above <https://care-navigation-admin-fe.int.eu.enterprise.ada.com> URL to do the scan.

2. Information Gathering

2.1.Amass

- Scan Using Amass

```
(user@user)-[~]
$ sudo amass enum -d care-navigation-fe.int.eu.enterprise.ada.com
care-navigation-fe.int.eu.enterprise.ada.com

OWASP Amass v3.23.2 (Critical or Exceptional Issue) https://github.com/owasp-amass/amass
Forward

1 names discovered - dns: 1

ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
Program IP 2606:4700:4400::/48 2 Subdomain Name(s)
172.64.144.0/20 1 Subdomain Name(s)
104.16.0.0/14 1 Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```

2.2. Knockpy

- Using Knockpy

```
(user@user)-[~] tools - Kali Docs - Kali Forums - Kali NetHunter - Exploit-DB - Google
$ knockpy care-navigation-fe.int.eu.enterprise.ada.com

v6.1.0

Domains

TIER TYPE
local: 10757 | remote: 1 All All
Wordlist: 10758 | Target: care-navigation-fe.int.eu.enterprise.ada.com | Ip: 172.64.146.211
10:51:42
login.cm.com
Ip address Code Subdomain Server Real hostname
*.ticketing.cm.com
Login to your account and go to https://www.cm.com/en-gb/app/ticket
(ctrl+c) | 0.0% | 0.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 0.00% | 01.care-navigation-fe.int.eu.enterprise.ada.com
Make sure to take a look at the user-side ticket store as well (https://sto
(ctrl+c) | 0.01% | 02.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 0.02% | 03.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 0.03% | 080.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 0.04% | 09.care-navigation-fe.int.eu.enterprise.ada.com
api.cmtelecom.com
(ctrl+c) | 0.05% | 1.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 0.06% | 10.care-navigation-fe.int.eu.enterprise.ada.com
```

```
(ctrl+c) | 99.8% | zsjy.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.8% | zpanel.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.8% | zs.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zt.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zulu.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zx.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zw.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zurich.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zy.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zyz.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zz.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zzz.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zzb.care-navigation-fe.int.eu.enterprise.ada.com
```

11:05:06

Ip address: 0 | Subdomain: 0 | **elapsed time: 00:13:23**

2.3. Dmitry

```
(user@user)-[~/Documents/Programs/rapidscan-master] val - Server Wide
$ sudo dmitry care-navigation-admin-fe.int.eu.enterprise.ada.com all
Deepmagic Information Gathering Tool SQL Injection
"There be some deep magic going on" File Upload
a Authentication Bypass
b Software Identification
HostIP:172.64.146.211
HostName:care-navigation-admin-fe.int.eu.enterprise.ada.com
d Webservice

Gathered Inet-whois information for 172.64.146.211 - Console
Reverse Tuning Options (i.e., include all except specified)
-timeout+ Timeout for requests (default 10 seconds)
-Userdbs Load only user databases, not the standard databases
inetnum: 171.34.0.0 - 172.80.127.255 standard dbs and load only user dbs
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK lb tests and load udb_tests
descr: userager IPv4 address block not managed by the RIPE NCC
remarks: until
remarks: url+ Target host/URL (alias of -host)
remarks: usecookie+ For registration information, responses in future requests
remarks: useproxy+ you can consult the following sources: to.conf, or argument http://server:port
remarks: version+ Print plugin and database versions
remarks: host+ IANA Virtual host (for Host header)
remarks: ipcode+ http://www.iana.org/assignments/ipv4-address-space responses (always). Format is
remarks: ipastr+ http://www.iana.org/assignments/iana-ipv4-special-registry negative response (
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks: AFRINIC (Africa)
remarks: user+ http://www.afrinic.net/ whois.afrinic.net
remarks: ipcode+ http://www.ubisoft.com
remarks: 2.5.0 APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: le IPs found: 3,232,151.32, 18,208,97,193, 18,209,196.61, 34,203,166.98, 34,196,34.1
remarks: IP+ ARIN (Northern America)
remarks: Hostname+ http://www.arin.net/ whois.arin.net
remarks: Ports+ 443
remarks: LACNIC (Latin America and the Carribean)
remarks: ip+ http://www.lacnic.net/ whois.lacnic.net
remarks: ciphers+ TLS_AES_128_GCM_SHA256
remarks:
country: time+ EU # Country is really world wide
admin-c: IANA1-RIPE
tech-c: nginx IANA1-RIPE
status: anti-c+ ALLOCATED UNSPECIFIED 1000 Location header is not present. See: https://developer.mozilla.org/en-US/docs/HTTP/Location
mnt-by: site up RIPE-NCC-HM-MNT strict-transport-security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/HTTP/Strict-Transport-Security
created: X-Content+ 2019-01-07T10:48:46Z 1000 Content-Type header is not set. This could allow the user agent to render
last-modified: 2019-01-07T10:48:46Z
source: page 2 re RIPE is to: https://www.ubisoft.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
role: Internet Assigned Numbers Authority
```

```

admin-c:      IANA1-RIPE
tech-c:      IANA1-RIPE
nic-hdl:     IANA1-RIPE
remarks:     For more information on IANA services
remarks:     go to IANA web site at http://www.iana.org.
mnt-by:      RIPE-NCC-MNT
created:     1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source:      RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.108 (BUSA)

timeout:     Timeout for requests (default 10 seconds)
depth:       Depth of look database, not the standard database

Gathered Inic-whois information for care-navigation-admin-fe.int.eu.enterprise.ada.com
ERROR: Unable to locate Name Whois data on care-navigation-admin-fe.int.eu.enterprise.ada.com

Gathered Netcraft information for care-navigation-admin-fe.int.eu.enterprise.ada.com
Retrieving Netcraft.com information for care-navigation-admin-fe.int.eu.enterprise.ada.com
Netcraft.com Information gathered

Gathered Subdomain information for care-navigation-admin-fe.int.eu.enterprise.ada.com
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host care-navigation-admin-fe.int.eu.enterprise.ada.com, Searched 0 pages containing 0 result
Gathered E-Mail information for care-navigation-admin-fe.int.eu.enterprise.ada.com

Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host care-navigation-admin-fe.int.eu.enterprise.ada.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 172.64.146.211

Port      State
25/tcp    open
80/tcp    open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed
All scans completed, exiting

```

3. Scanning Vulnerability

3.1. Scanning ports using Nmap

```
(user@user)-[~]
$ sudo nmap -sS 172.64.144.0
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 03:59 PDT
Nmap scan report for 172.64.144.0
Host is up (0.068s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 71.65 seconds
```

3.2. Scan with rapid scan.

Check out our new software, [NetBot](https://github.com/skavngr/netbot) for simulating DDoS attacks - <https://github.com/skavngr/netbot>

- Some ports are open.

Vulnerability Threat Level	Low Some ports are open. Perform a full-scan manually.
Vulnerability Definition	Open Ports give attackers a hint to exploit the services. Attackers try to retrieve banner information through the ports and understand what type of service the host is running
Vulnerability Remediation	It is recommended to close the ports of unused services and use a firewall to filter the ports wherever necessary. This resource may give more insights: https://security.stackexchange.com/a/145781/6137

- SNMP service Detected.

Vulnerability Threat level
Medium SNMP Service Detected.

Vulnerability Definition
 Hackers will be able to read community strings through the service and enumerate quite a bit of information from the target. Also, there are multiple Remote Code Execution and Denial of Service vulnerabilities related to SNMP so [check](#).

Vulnerability Remediation
 Use a firewall to block the ports from the outside world. The following article gives wide insight on locking down SNMP service, <https://www.techrepublic.com/article/lock-it-down-dont-allow-snmp-to-compromise-network-security/>

- X-XSS Protection is not Present.

```
Vulnerability Threat Level
medium X-XSS Protection is not Present
Vulnerability Definition
As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.
```

- Found Subdomains with Amass

```
Vulnerability Threat Level
medium Found Subdomains with Amass
Vulnerability Definition
Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

- RDP Server Detected over UDP.

```
Vulnerability Threat Level
high RDP Server Detected over UDP.
Vulnerability Definition
Attackers may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing the password on the target.
Vulnerability Remediation
It is recommended to block the service to outside world and made the service accessible only through the a set of allowed IPs only really necessary. The following resource provides insights on the risks and as well as the step to block the service. https://www.perspectiverisk.com/remote-desktop-service-vulnerabilities/
```

4. Vulnerability description.

- SNMP Service Detected: An SNMP service has been identified, which could potentially pose a security risk due to its exposure and could lead to unauthorized access or information disclosure.
- X-XSS Protection is not Present: The absence of XSS protection in a web application or website means that it may be vulnerable to cross-site scripting attacks, potentially allowing attackers to inject malicious scripts into web pages.
- Found Subdomains with Amass: Subdomains have been discovered using the Amass tool, which may indicate a potential attack surface expansion or information exposure risk.
- RDP Server Detected over UDP: The presence of an RDP server running over the UDP protocol can pose security risks and may result in vulnerabilities in remote desktop access.

5. Affected components.

- Network devices and services using SNMP.
- Web application or website without XSS protection.
- Domain and its subdomains.
- RDP server and remote access services.

6. Impact assessment.

- SNMP Service Detected: Potential unauthorized access to network devices and potential data leaks.
- X-XSS Protection is not Present: Risk of cross-site scripting attacks, potentially leading to data theft or unauthorized actions on the web application.
- Found Subdomains with Amass: Information exposure, potential for subdomain-related vulnerabilities.
- RDP Server Detected over UDP: Vulnerabilities in the RDP service and possible compromise of remote access.

7. Steps to reproduce.

None.

8. Proof of concept (if applicable)

None.

9. Proposed mitigation or fix

- SNMP Service: Restrict SNMP access and use strong community strings. Update and patch SNMP configurations.
- X-XSS Protection: Implement proper input validation and output encoding to protect against cross-site scripting.
- Subdomains: Carefully manage and secure discovered subdomains to prevent information exposure.
- RDP Server: Review and secure RDP server configurations. Consider avoiding UDP for sensitive environments.

10. Summary

Multiple vulnerabilities have been identified, including potential SNMP service risks, the absence of XSS protection in a web application, expanded attack surface with discovered subdomains, and RDP server vulnerabilities. Mitigation measures and thorough security assessments are necessary to protect the affected components and ensure system security.