{{ client }}

{{ contract }}

{{ month }} {{ year }}

Audit Report

Summary

[1. Introduction 2](#_Toc42014144)

[1.1 Audit context 2](#_Toc42014145)

[2. Synthesis 3](#_Toc42014146)

[2.1 Global security level 3](#_Toc42014151)

[2.2 Security defects 3](#_Toc42014152)

[3. Security defects summary 4](#_Toc42014153)

[4. Corrective actions summary 5](#_Toc42014154)

[5. Details of the security defects and corrective actions 6](#_Toc42014155)

[6. Annexes 7](#_Toc42014156)

[6.1 Vulnerabilities evaluation scale 7](#_Toc42014163)

[6.2 Open services 8](#_Toc42014164)

# Introduction

## Audit context

Project owner: {{ owner.name }} {{ owner.surname }} – {{ owner.email }}

Pentesters :

|  |  |
| --- | --- |
| **Name** | **Email** |
| {%tr for pentester in pentesters %} |  |
| {{ pentester.surname }} {{ pentester.name }} | {{ pentester.email }} |
| {%tr endfor %} |  |

The audit perimeter can be listed as follows:

{%p for scope in scopes %}

{{ scope.scope }}

{%p endfor %}

# Synthesis



## Global security level

Todo

## Security defects

During this audit, **{{ defects|count }} security defects** were found:

|  |  |  |  |
| --- | --- | --- | --- |
| Critical : **{{ defects | selectattr('risk','equalto', 'Critical')|list|count }}** | Major : **{{ defects | selectattr('risk','equalto', 'Major')|list|count }}** | Important : **{{ defects | selectattr('risk','equalto', 'Important')|list|count }}** | Minor : **{{ defects | selectattr('risk','equalto','Minor')|list|count }}** |

The evaluation of their criticity is based on the standard evaluation scale suggested by the French ANSSI agency (Agence Nationale de la Sécurité des Systèmes d’Information).

{%p if positive\_remarks | count is ge 1 %}

## Positive remarks

{%p for positive\_remark in positive\_remarks %}

* {{ positive\_remark }}

{%p endfor %}

{%p endif %}

{%p if negative\_remarks | count is ge 1 %}

## Bad practices

{%p for negative\_remark in negative\_remarks %}

* {{ negative\_remark }}

{%p endfor %}

{%p endif %}

{%p if neutral\_remarks | count is ge 1 %}

## Vigilance point

{%p for neutral\_remark in neutral\_remarks %}

* + {{ neutral\_remark }}

{%p endfor %}

{%p endif %}

# Security defects summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Title** | **Exploitation** | **Impact** | **Type** |
| **{%tr for x in defects|selectattr('risk','equalto', 'Critical') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate }} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Major') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate }} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Important') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate}} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Minor') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate }} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |

*Type: B = Base, A = Application, D = Data, P = Security policy*

*The detail of the evaluation scale is provided in the Annexes.*

# Corrective actions summary

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Title** | **Implementation** | **Gain** |
| **{%tr for fix in fixes %}** |  |  |  |
| **A{{ fix.id }}** | {{ fix.title }} | **{% cellbg colors.fix[fix.execution] %}{{ fix.execution|translate }}** | **{% cellbg colors.fix[fix.gain] %}{{ fix.gain|translate }}** |
| **{%tr endfor %}** |  |  |  |

***Details of the criteria « Implementation »***

*Quick Win: asset configuration, sanitizing of input(s)*

*Moderate: limited code changes, implementation of a security component*

*Major: extensive changes within the code or the architecture of the asset*

# Details of the security defects and corrective actions{% for x in defects|selectattr('risk','equalto', 'Critical') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for instance in x.instances %}

{%p for para in instance.notes\_paragraphs %}

{{ para }}

{%p endfor %}

{%p for proof in instance.proofs %}

{{ proof }}

{%p endfor %}

{% endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Implementation* | *Gain* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}{% for x in defects|selectattr('risk','equalto', 'Major') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for instance in x.instances %}

{%p for para in instance.notes\_paragraphs %}

{{ para }}

{%p endfor %}

{%p for proof in instance.proofs %}

{{ proof }}

{%p endfor %}

{% endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Implementation* | *Gain* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for instance in x.instances %}

{%p for para in instance.notes\_paragraphs %}

{{ para }}

{%p endfor %}

{%p for proof in instance.proofs %}

{{ proof }}

{%p endfor %}

{% endfor %}

{% endfor %}{% endfor %}{% for x in defects|selectattr('risk','equalto', 'Important') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for instance in x.instances %}

{%p for para in instance.notes\_paragraphs %}

{{ para }}

{%p endfor %}

{%p for proof in instance.proofs %}

{{ proof }}

{%p endfor %}

{% endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Implementation* | *Gain* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}{% for x in defects|selectattr('risk','equalto', 'Minor') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for instance in x.instances %}

{%p for para in instance.notes\_paragraphs %}

{{ para }}

{%p endfor %}

{%p for proof in instance.proofs %}

{{ proof }}

{%p endfor %}

{% endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Implementation* | *Gain* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}

# Annexes



## Vulnerabilities evaluation scale

The vulnerabilities identified during the audit are evaluated according to the standard scale proposed by the French ANSSI agency (Agence Nationale de la Sécurité des Systèmes d’Information).

They are sorted according to the risk they cast on the information system, that is to say, the impact of the exploitation of the vulnerability as well as its complexity of execution by an attacker.

Exploitation:

* **Easy:** trivial exploitation, without any particular tool;
* **Moderate:** the exploitation requires simple techniques and publicly-available tools;
* **Difficult:** the exploitation requires advanced knowledge in information systems security as well as coding simple tools such as scripts;
* **Arduous:** the exploitation of 0-day vulnerabilities that requires an, expertise in information systems security as well as coding various, complex, targeted tools.

Impact:

* **Minor:** no direct consequences on the security of the audited perimeter;
* **Important:** isolated consequences on the security of the audited perimeter;
* **Major:** limited consequences on the security of some parts of the audited perimeter;
* **Critical:** extensive consequences on the security of the whole audited perimeter.

Resulting risk:

* **Minor:** minor risk that might require a fix;
* **Important:** moderate risk that requires a fix in the medium term;
* **Major:** major risk that requires a fix in the short term;
* **Critical:** critical risk that requires an immediate fix or the shutdown of the perimeter.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **↓ Impact Exploit. →** | **Arduous** | **Difficult** | **Moderate** | **Easy** |
| **Minor** | Minor | Minor | Important | Major |
| **Important** | Minor | Important | Important | Major |
| **Major** | Important | Major | Major | Critical |
| **Critical** | Important | Major | Critical | Critical |

## 

## Open services

The table below summarizes the available services on each open port of every IP within the audited perimeter, with our comment.

|  |  |  |  |
| --- | --- | --- | --- |
| Hosts | Port | Service | Notes |
| {%tr for port in ports %} |  |  |  |
| {{ port.ip }} | {{ port.port }}/{{ port.proto }} | {{ port.service }} | {{ port.product }} |
| {%tr endfor %} |  |  |  |