Audit certificate

Context

Helvetic Payroll has asked Synacktiv to perform an independent security assessment of the Puma application and the internet facing resources of Helvetic Payroll.

The assessment was performed on the production environment following a grey-box methodology (accounts of different privileges were given to the auditors). The objectives were to identify vulnerabilities affecting Helvetic Payroll's infrastructure and evaluate the associated risks.

The following documents were used to conduct this assessment:

- ISO 19011
- OWASP Testing Guide

Engagement scope

The engagement scope was:

- The Puma application.
- The internet facing IP addresses given to the auditors prior to the tests.

The audit was performed from Helvetic Payroll offices from the 21st to the 25th of August 2023. Two counter audits of the corrective measures implemented were then carried out on Synacktiv's premises from the 2nd to the 3rd of April 2024 and the 3rd of July 2024.

Results

The tests performed by Synacktiv experts during the assessment revealed a high security level.

- Synacktiv identified 16 security issues during the initial assessment.
- The first counter audit revealed 3 remaining vulnerabilities, 2 of medium severity and 1 of low severity.
- All vulnerabilities were fixed for the last counter audit.

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.

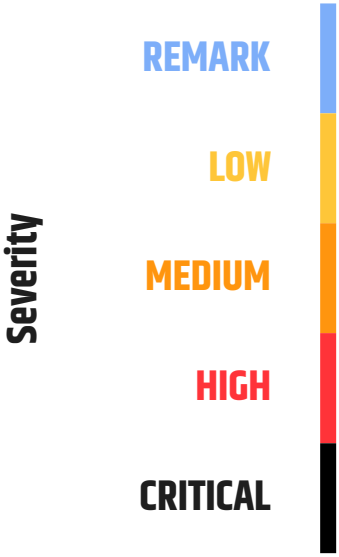
LOW

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.



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.