onvio.
information security

advisory report
pentest.

Currence iDEAL B.V.

Thursday, July 4, 2024

CONFIDENTIAL

Utrecht, Thursday, July 4, 2024

Currence iDEAL B.V.
Attn. I. Spiliopoulos
Omval 300
1096HP, Amsterdam
Nederland

Document
Reference: IDL
Version: 1.0
Classification: Client
Team:
Dick Snel
Jasper Weijts
Osman Hussein
Joep van Antwerpen
Andreas Damen

Service: API Blackbox / Greybox Pentest and Configuration/ Cloud Reviews

As a result of the conducted pentest on iDeal on behalf of Currence iDEAL B.V., Onvio presents her findings in this advisory report.

Warning

Onvio B.V.
Churchilllaan 11
3527 GV, Utrecht
The Netherlands

www.onvio.nl
info@onvio.nl

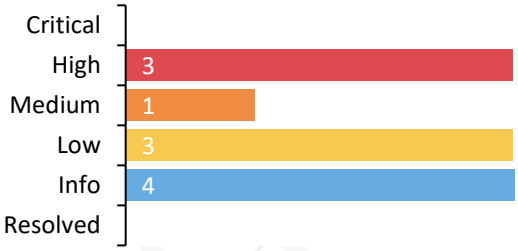
VAT-ID | NL853511901B01
CoC | 59476486
IBAN | NL12INGB0007300606

Management summary

Onvio has drawn up a risk profile as a result of the Overview of all findings. This profile gives an immediate insight into the risk and impact of the findings.

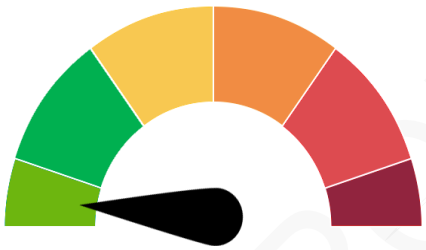
Perspective: From the Internet without supplied account.

Risk score 5 of 6

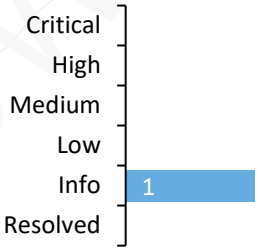


Number of findings on risk classification

Perspective: From supplied source code.



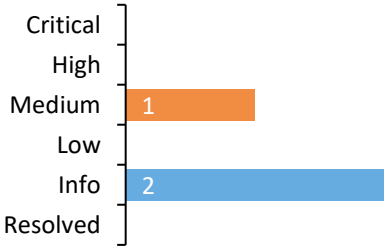
Risk score 1 of 6



Number of findings on risk classification

Perspective: From inside the MongoDB Cloud with supplied account.

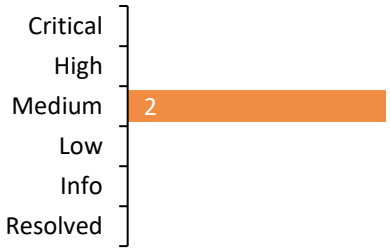
Risk score 4 of 6



Number of findings on risk classification

Perspective: From inside CloudFlare with supplied account.

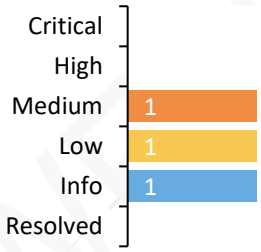
Risk score 4 of 6



Number of findings on risk classification

Perspective: From inside AWS/EKS with supplied account.

Risk score 4 of 6



Number of findings on risk classification

Risk score 1 = Very strong, 6 = Very weak

Critical
A direct threat to security with a high impact. Mitigate these risks immediately.

High
An important risk that probably leads to intrusion and loss of data. Urgent mitigating.

Medium
Tied to conditions, if combined, they may lead to high risks. Mitigate in the short term.

Low
Often used to find entries into the objects. Mitigate in the medium term.

Informational
Informative findings do not constitute a direct threat, but are for the information of the client.

Resolved, accepted or no risks found
No risks have been found, or they have been resolved or accepted.

Findings from the perspective without an account, can automatically be abused with an account. Risk score is classified based on the CVSS v3.1 system.

Findings and recommendations

The following key findings can be identified:

Perspective: From the internet without supplied account

- A malicious user can possibly reveal the secret information used to create a session token. The risk of this is that if a malicious user is able to reveal the secret information. They could create and sign their own session tokens.
- Malicious users can discover valid email addresses. This information can be used in the execution of other attacks like phishing.
- A malicious user can bypass the Multi Factor timeout functionality on multiple locations. The risk of this is that a malicious user can perform more tries and in the worst case, for example, increase the chances of guessing the correct code.

Perspective: From inside AWS/EKS with supplied account

- The Amazon Elastic Block Store (EBS) volumes for Kubernetes are not encrypted. The risk of this is that a malicious user can get access to possibly sensitive information that is stored.
- Kubernetes clusters do not have "Secrets encryption" enabled. The risk of this is that a malicious user is able to read plaintext stored secrets from etcd in Kubernetes Secrets. These secrets can be used to make authenticated requests to certain services.

Perspective: From inside CloudFlare with supplied account

- An anonymous user can gain access to the Payconiq Atlassian Servicedesk and request access to critical resources. If the request is approved, a malicious person can get access to critical resources.
- DNS records in CloudFlare do not resolve to an IP or existing host anymore. The risk of this is that sub-domains can be taken over. These can then be used for evil purposes by a malicious person, for example phishing.
- CloudFlare Web Application Firewall (WAF) rules can be bypassed. The risk of this is that a malicious person can bypass these rules and, for example, successfully perform Brute-Force attacks on login pages.
- The managed rules used in CloudFlare are not up-to-date. The risk of this is that a malicious person can bypass the Web Application Firewall (WAF) and successfully perform certain attacks.

Perspective: From inside the MongoDB Cloud with supplied account

- Multiple high privileged user accounts do not have Multi Factor Authentication (MFA) enabled. The risk of this is that when a malicious user captures the password of one of these high privileged user accounts, he would have direct access to it.

Perspective: Retested findings from previous reports

ID	Risk	Retested	Status	Description
3200-01	MEDIUM	Yes	Fixed	E-mail verification can be skipped using another endpoint
3200-02	MEDIUM	Yes	Fixed	Active deprecated endpoint bypasses e-mail verification
3200-03	LOW	Yes	Fixed	E-mail comparison can be bypassed using homoglyphs
3200-04	LOW	Yes	Open	E-mails in default aliases are not masked
3200-05	LOW	Yes	Open	Verbose errors are shown to end user
3200-06	LOW	No	Open	AWS temporary access tokens displayed
0324-01	MEDIUM	Yes	Open	Outdated and vulnerable dependencies in use
0324-02	LOW	No	Open	Docker does not instruct to lower privileges
0324-03	LOW	No	Open	Docker socket exposed

Positive findings

- Both the Cloud environments were not reachable without the use of a VPN, meaning they are protected well against outsider threats.
- MongoDB | The MongoDB instances make use of Encryption at Rest. Making the data more secure, and less likely to be stolen by malicious users.
- MongoDB | The MongoDB instances make use of at least TLS 1.2. Making the transport of data very secure, and the chance of data being stolen even smaller.
- API | Session tokens expire quickly, making abuse unlikely.

The following key recommendations can be identified:

- Atlassian | Make sure only whitelisted domains are allowed to register with the website.
- CloudFlare | Remove not resolving records and implement a policy to periodically check for stale records. Monitor for subdomain takeovers.
- CloudFlare | Check if rules are implemented correctly and can't be bypassed.
- API | Make sure a new nonce is used every time a new token is signed. This prevents malicious users from recovering the nonce and private key.
- MongoDB | Ensure that all users, or at least accounts with high privileges, are required to complete an MFA process before a user can successfully log in.
- EKS | Enable and enforce EBS encryption by default.

The following peculiarities occurred during the investigation:

- No access was provided to the MongoDB/Kubernetes (kubectl) clusters themselves. Only access to the dashboards was supplied. This severely limited the thoroughness of the investigations.
- Whitelisting of the Onvio IP addresses on the Currence issuer and acquirer API was resolved after one week of testing.

Conclusion

The aim of this Pentest is to gain a clear insight into the current security level of the Payconiq iDeal Payment gateway, in specific the new profile functionalities, and the environment in which it operates. Security risks and vulnerabilities must be identified. The results of this research will help Currence and Payconiq to make improvements and raise security to a higher level.

By identifying vulnerabilities, security and privacy risks must be mitigated. This creates greater certainty about the reliability, security and integrity of the system and the data stored within it.

The findings and recommendations of the investigation, together with further details that have occurred during the execution of this test, lead to the conclusion that the objects of investigation need improvements in security measures to make them more resilient to an attacker.

The research questions can be answered as follows:

- Within the CloudFlare environment, **three high** and **two medium** classified risks have been identified.
- Within the EKS environment, **one medium**, **one low** and **one informational** classified risk have been identified.
- Within the MongoDB environment, **one medium** and **two informational** classified risks have been identified.
- At the API level, **one medium**, **two low** and **three informational** classified risks have been identified.
- At the web level, **one low** and **one informational** classified risk have been identified.
- At the code level, **one informational** classified risk has been identified.
- No deficiencies were found in restricting rights amongst users.
- The current state of hardening of EKS, MongoDB, CloudFlare and the API's is **insufficient**.

onvio.
information security

Table of Contents

Introduction

The client wants to gain insight into the current security level of the newly implemented iDeal functionalities with the goal of improving security. See the "Objective" section for a detailed description of the stated objectives.

To this end, the client asked Onvio to conduct an API Pentest, Cloudflare/MongoDB and EKS Configuration review to investigate the security of the newly developed iDeal profile implementation. During the execution of this investigation, all identified risks were carefully recorded and documented in this final result of the investigation.

The management summary gives the general impression of the security level of the investigated objects, followed by an overview of the key findings and their impact. Finally, recommendations are made for resolving issues and avoiding them in future.

The technical documentation gives a description of each identified risk. How a vulnerability was found, how it works, what the impact is, how high the risk is that it will be exploited and how the issue can be mitigated. This practical documentation allows a developer to mitigate risks effectively.

This document will be given to the client digitally by e-mail as an encrypted attachment. After approval by the client, Onvio will destroy its copies of this document and all other data relating to the execution of this test. It is recommended that the full report should be kept carefully; this information can then be re-used by Onvio to ensure that any repeat tests can be done more efficiently.

Investigation and scope

Purpose

The aim of this Pentest is to gain a clear insight into the current security level of the Currence iDeal Payment gateway, in specific the profile functionalities, and the environment in which it operates. Security risks and vulnerabilities must be identified. The results of this research will help Currence and Payconiq to make improvements and raise security to a higher level.

By identifying vulnerabilities, security and privacy risks must be mitigated. This creates greater certainty about the reliability, security and integrity of the system and the data stored within it.

In order to achieve the set goal, Onvio's will carry out the API Pentest, Cloudflare/MongoDB and EKS Configuration review service. The investigations are carried out by "legal" hackers with knowledge of current security solutions and risks. These specialists carry out extensive research using automated tools as well as manual inspections.

The investigation will identify shortcomings and vulnerabilities and identify and classify the resulting risks in an advisory report.

Objects investigated

The following objects have been defined as in scope for the project:

IP Range, domain or application	Description
Black/Greybox Pentest - Payconiq iDeal Payment gateway EXT Environment URLs https://acquirer.ext.idealapi.nl/v2 https://issuer.ext.idealapi.nl/v2 https://ext.profile.ideal.nl/ https://ext.pay.ideal.nl/api/v1 API specs ideal-profile-management-bff-api-master.zip ideal-issuer-api-master.zip ideal-acquirer-api-master.zip Postman collection ideal-postman-collections-master.zip	The external API's used by issuers and acquirers. Examined from the perspective of an anonymous visitor and a user with a valid but rights-limited account.
Cloudflare - Review manual & Terraform settings/config URL https://dash.cloudflare.com/ Account j.weijts@onvio.nl	Cloudflare - Review manual & Terraform settings/config
EKS - Review current state of hardening URL https://d-99671d3cdd.awsapps.com/start/#/?tab=accounts Account onvio.pentest@payconiq.com	EKS - Review current state of hardening
Cloudflare - MongoDB Review URL https://account.mongodb.com/account/login Account onvio.pentest@payconiq.com	MongoDB - Review current state of hardening

During the investigation, only objects at the above locations were examined. Check the accounts that were used and remove them from systems and applications, including any remaining test data.

Out of scope

The following work and activities are considered beyond the scope of this project:

- Performing social engineering attacks is excluded from this investigation.
- Performing a source code review is excluded from this study.

Research questions

After determining the purpose and research objects for this project, the following research questions can be formulated, which this investigation should attempt to answer:

- What vulnerabilities can be found in the application(s) and infrastructure that are accessible via the internet, both with and without a valid user account.
- Can any vulnerabilities at the application level be discovered?
- Can any vulnerabilities at the server level be discovered?
- Are users restricted in their rights?
- What is the current state of hardening of EKS and CF?

Documents and information supplied

The client has supplied the following documents and information for the execution of the project:

- 29/04 Scope Meeting
- 03/05 Api Documentation
- 06/05 Scope Meeting
- 07/05 Kubernetes Platform Architecture
- pentest-resources.zip-2024-5-27 11.23.46.zip
- email-verification-flow.png
- 0324-004 Security assessment iDEAL 2.0.pdf-2024-6-3 9.31.6.pdf
- 3200-006 Security assessment iDEAL platform.pdf

All work done from Onvio's office location will be done from the IP address: 157.97.115.170, 128.199.55.141, 188.166.109.219, 167.71.4.231.

Team and contacts

Given the specialism and the significance of a thorough security test, a permanent experienced team has been set up for the execution of this project. This project will be led by Jasper Weijts, also the primary contact person assigned to this project.

The team for the execution of this assignment is as follows:

Jasper Weijts
Senior security specialist

Email | j.weijts@onvio.nl
Mobile | +31 (0)6 20 70 44 73
www.linkedin.com/in/jasper-weijts

Certifications:
OSWE, OSWP, OSCE, OSCP, CEH, SLAE

Screening:
ID, VOG, Antecedenten, AIVD-B

Andreas Damen
Medior security specialist

Email | a.damen@onvio.nl
Mobile | +31 (0)6 80 18 31 53
linkedin.com/in/andreas-damen/

Certifications:
OSCP, OSWA, BSCP, eWPTXv2, MAPT, eWPT, eJPT

Screening:
ID, VOG, Antecedenten

Joep van Antwerpen
Medior security specialist

Email | j.vanantwerpen@onvio.nl
Mobile | +31 (0)6 14 21 10 56
www.linkedin.com/in/joep-va

Certifications:
BSCP, OSWE, OSCP, eWPTX, eWPT, eJPT

Screening:
ID, VOG, Antecedenten

Osman Hussein
Security specialist

Email | o.hussein@onvio.nl
Mobile | +31 (0)6 27 14 69 20
www.linkedin.com/in/osman-hussein-136684198/

Certifications:
OSCP, BSCP, BSc, AZ 900, AZ 104, AZ 500

Screening:
ID, VOG, Antecedenten

Dick Snel
Senior security specialist

Email | d.snel@onvio.nl
Mobile | +31 (0)6 12 42 66 93
www.linkedin.com/in/dick-snel

Certifications:
OSCE, OSCP, OSWE, CISSP, CISM, CEH, CCSP

Screening:
ID, VOG, Antecedenten, AIVD-B, Banker's Oath

The CVs of the individual team members can be requested from Onvio, as well as their VOG (declaration of good conduct); the certificates and IDs of all team members are available for inspection. All team members are highly experienced seniors and Certified Ethical Hackers (CEH) and are OSCP certified (Offensive Security Certified Professional).

Project management and planning

This project is being managed by an experienced team to ensure the quality, organization, administration and communication.

Onvio offers as much flexibility as possible in the execution of the project. A lead time is determined for projects. During the intake, the exact days on which the actual testing on the systems of the Client will be carried out will be recorded.

Duration project:	*16 days*
Start project:	*Monday, June 3, 2024*
End project:	*Thursday, July 4, 2024*
Delivery:	*Thursday, July 11, 2024*

Guarantee and completeness

The client must be aware that the results of security tests do not provide guarantees for the future and that the absolute security of systems and organizations can never be guaranteed. The client is also aware that not all unknown errors within existing software can necessarily be detected within the agreed term. Onvio can therefore not be held liable for this.

Findings

This technical summary is intended for developers, programmers or vendors. With this practical information, the findings of this report can be solved. Where necessary, Onvio is available to provide further clarification.

Risk classification according to CVSS v3.1

The industry-standard Common Vulnerability Scoring System CVSS version 3.1 is used to classify the severity of findings. The CVSS system produces a risk score for each finding from zero (0) to ten (10), with ten being the highest risk. This score is classified according to the table below:

Classification	CVSS Score
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Informational	0.0

For each finding, the CVSS parameters are included which collectively form the so-called 'Vector' string.

With the Vector, the creation of the score is transparent and can be easily reproduced.

The following notes apply to the classifications:

Critical
A direct threat to security with a high impact. Mitigate these risks immediately.

High
An important risk that probably leads to intrusion and loss of data. Urgent mitigating.

Medium
Tied to conditions, if combined, they may lead to high risks. Mitigate in the short term.

Low
Often used to find entries into the objects. Mitigate in the medium term.

Informational
Informative findings do not constitute a direct threat, but are for the information of the client.

Resolved, accepted or no risks found
No risks have been found, or they have been resolved or accepted.

Logs

Extensive logs are accumulated during the testing. This information has been used for drawing up this report and has been stored in the dossier for this project. In any event, this information is stored for a limited period on the systems of Onvio until the client gives instructions to destroy it, as stated in the scope.

Overview of all findings

Per finding a fixed pattern is explained what the finding entails, what the risks are and how it can be prevented by means of a recommendation.

The following chapters describe each finding in detail.

Perspective: From the Internet without supplied account

ID	Finding	Risk	Status
IDL-H-01	CloudFlare | Servicedesk is publicly accessible	HIGH - 8.2	New
Make sure only whitelisted domains are allowed to register with the website.			
IDL-H-02	Cloudflare | DNS records do not resolve and result in subdomain takeover	HIGH - 7.5	New
Remove not resolving records. Implement a policy to periodically check for stale records. Monitor for subdomain takeovers.			
IDL-H-03	Cloudflare | Web Application Firewall (WAF) can be bypassed	HIGH - 7.5	New
Use lower() in all expressions the make sure checks are case insensitive.			
IDL-M-04	API | JSON Web Token ES256 Secret key and nonce can possibly be revealed	MEDIUM - 6.5	New
Make sure a new nonce is used every time a new token is signed. This prevents malicious users from recovering the nonce and private key.			
IDL-L-09	Web | Web applications are missing some security headers settings	LOW - 3.7	New
Consider implementing available HTTP security headers as a way to improve overall Web site security.			
IDL-L-10	API | User names can be retrieved via registration	LOW - 3.7	New
Ensure that notifications to end users never disclose more information than is strictly necessary. Display generic messages from which it is not possible to tell whether a username is correct. Implement a CAPTCHA on the registration form to prevent automatic retrieval of usernames.			
IDL-L-11	API | Timeouts on multi factor attempts can be bypassed	LOW - 3.1	New
Improve the timeout/lockout mechanism so that it also remembers which email addresses have been temporarily locked out.			

IDL-I-13	Web | Web application uses software with vulnerabilities	INFO - 0.0	New
Ensure that unused software is removed to avoid unnecessary risk. If the software does be used, care must be taken to ensure that it is up-to-date.			
IDL-I-14	API | Verbose errors are shown to end user	INFO - 0.0	New
Ensure that error messages to end users on production systems never disclose more information than is strictly necessary. Display generic error messages.			
IDL-I-15	API | Encryption algorithms and ciphers insufficiently strong	INFO - 0.0	New
Support only communication over at least TLS1.2 with strong ciphers.			
IDL-I-16	API | E-mails in default aliases are not masked	INFO - 0.0	New
Determine whether it is necessary to mask the aliases of profiles or change the default value of aliases.			

Perspective: From supplied source code

ID	Finding	Risk	Status
IDL-I-20	Code | Dependencies with known vulnerabilities	INFO - 0.0	New
Make sure unused dependencies are removed to avoid unnecessary risk. Make sure necessary dependencies are up-to-date.			

Perspective: From inside the MongoDB Cloud with supplied account

ID	Finding	Risk	Status
IDL-M-08	MongoDB | High privileged accounts without Multi Factor Authentication (MFA) set up	MEDIUM - 4.2	New
Ensure that all users, or at least accounts with high privileges, are required to complete an MFA process before a user can successfully log in.			
IDL-I-17	MongoDB | Old MongoDB version used by multiple clusters	INFO - 0.0	New
Ensure that the clusters running the old MongoDB version are updated to a newer before version 5.0 reaches EOL.			
IDL-I-18	MongoDB | AWS encryption key needs rotation	INFO - 0.0	New
Rotate the key in order to better secure the stored data.			

Perspective: From inside CloudFlare with supplied account

ID	Finding	Risk	Status
IDL-M-05	Cloudflare | Web Application Firewall (WAF) certificate check can be bypassed	MEDIUM - 6.5	New
Add a check for cf.tls_client_auth.cert_revoked.			
IDL-M-06	Cloudflare | Web Application Firewall (WAF) outdated rulesets	MEDIUM - 5.3	New
Update all WAF rulesets. Enable rule 100048.			

Perspective: From inside AWS with supplied account

ID	Finding	Risk	Status
IDL-M-07	EKS | EBS volumes for Kubernetes are not encrypted	MEDIUM - 4.3	New
Enable and enforce EBS encryption by default.			
IDL-L-12	EKS | Kubernetes secrets are stored in plaintext in etcd	LOW - 3.1	New
Apply secrets encryption in order to prevent them from being read and leaked.			
IDL-I-19	EKS | Old Kubernetes version used by cluster	INFO - 0.0	New
Ensure that the cluster running the old Kubernetes version is updated to a newer before version 1.27 reaches EOL.			