OnRobot A/S

Teglvaerksvej 47H
5220 Odense
Denmark
info@onrobot.com
onrobot.com

WEBLYTICS SECURITY OVERVIEW

About the report

This document is based on the results of security tests and reviews of the WebLytics software performed by Prueba Cybersecurity, an independent cybersecurity company.

'WebLytics Security Overview' is designed to provide an overview of the WebLytics installation and how WebLytics handles important security issues to provide a secure service to the end users.

Overview of WebLytics

WebLytics is a locally installed software that operates in the local network to collect metrics from the robots, OnRobot Compute Boxes and OnRobot tools. Furthermore, WebLytics provides an overview of hardware telemetries. Additionally, WebLytics is allowed to send alerts when specific metrics exceed user-defined ranges.

Administrators of the WebLytics installation can set up multiple users and use role-based access control and group-based device membership to control which functionality and information is available for each individual user.

Network Protection

The encryption level of the WebLytics web interface and API is determined by the configuration according to the customer's security demand. Furthermore, the service access is protected by a username and password access control. To strengthen login security, a strong minimum password requirement is enforced. Defensive measures, such as request throttling and anti-bot mechanisms, harden

and reduce the risk of attack. Upon successful authentication, WebLytics uses a securely signed and managed web token for session management. The token is safeguarded from client-side theft vulnerabilities.

Compliant telemetry collection

Telemetric data is collected by OnRobot on a regular basis for development and product improvement purposes. To ensure GDPR compliance with telemetric data, collected data samples from different hardware have been reviewed and shown not to contain any GDPR sensitive information. No user information from the WebLytics installation is collected.

External license and data server

The license and data server perimeters are externally secured so that the only ports open are those required for web communication with WebLytics installations and for license administration. Communication between a WebLytics installation and the external servers uses TLS encryption. This keeps all traffic safe and secure in transit.

All servers are protected with Multifactor Authentication, Antivirus, and Firewalls in a protected datacenter. The data is being stored at Microsoft's West European Azure datacenter in the Netherlands, which has achieved compliance with numerous standards including ISO27001:2013, NIST HIPAA, FedRAMP, SOC 1, and SOC 2. The facility itself is a level 4 datacenter, the highest in regards of security and SLA uptime.

General recommendations

Beyond the security implemented into the WebLytics product itself, a customer can increase their own security posture when handling WebLytics by following these recommendations:

- Segregate the network where WebLytics and hardware units are deployed and ensure that proper firewalling is in place.
- Use a password manager to generate random passwords and store them securely.
- Use up-to-date browsers to access the WebLytics web interface.
- Provide access to the WebLytics web interface via a private network connection or company VPN.
- Secure physical access to the WebLytics host machine.

Security tests and review

Prueba Cybersecurity is an independent cybersecurity company. The company performed rigorous security tests and review of the WebLytics platform before release. The security tests consisted of multiple phases including black box testing, grey box testing, architecture review, communication transport review and development pipelines. Prueba also conducted an external audit of the WebLytics security assessment and tested for compliancy with the CIS20 framework. (CIS20 compliancy is reviewed on an annual basis.)

Prueba Cybersecurity was given access to all required authentication and authorization data required to test the internal and external architecture of the WebLytics software platform, including transport communication and development.

Prueba Cybersecurity also had access to numerous OnRobot contacts throughout the process. OnRobot experts were able to supply information and access to all WebLytics systems, without creating any limitations that would hinder or obstruct Prueba Cybersecurity's security tests or reviews. Throughout the process, the identified issues and the received hardening recommendations were handled by an immediate fix or recognized and prioritized for fixing by OnRobot.

Prueba Cybersecurity understands that OnRobot is committed to fixing identified issues and to continuously delivering the required attention and improvements to secure and harden the WebLytics platform.

RESULT: Prueba Cybersecurity did not identify any critical security issues that would directly lead to the compromise of the customers WebLytics installation, host machine or network.