OpenSynergy’s Security Mission

Description

OpenSynergy’s Security Mission

What is a Security Vulnerability?

A security vulnerability is an unexpected flaw within an OpenSynergy software product that can be exploited to perform unauthorized actions. Unauthorized actions include unauthorized access to information or unauthorized modification of information.

OpenSynergyâ??s Commitment

Our mission is to provide products to our customers that are fit for purpose. OpenSynergy takes great care in the design and development of its software products, to avoid that the released products are subject to Security Vulnerabilities.

Nevertheless, Security Vulnerabilities might be present in released products and might come to our attention during internal analysis or from reports that we occasionally receive from our customers, our partners or independent research institutes.

We encourage all third parties to report Security Vulnerabilities directly to us following the process outlined in the Section â??Reporting a Security Vulnerabilityâ?•. We value every report communicated to us by customers, partners or third parties. We will assign the submitted report a tracking number and respond within four working days to acknowledge receipt of the report. We will evaluate the contents of the report and outline the next steps in the process. We are committed to being responsive and keeping reporters informed of our progress as we investigate and mitigate the reported security concern.

When it comes to disclosing Security Vulnerabilities, OpenSynergy is committed to following the Responsible Disclosure approach. This process has two steps: a confidential stage allowing our customers to understand and address the issue and a delayed public disclosure.

As soon as the Security Vulnerability has been analyzed and the security risk has been identified, we will inform the supported customers of the affected products (directly or via our distributors) disclosing the nature of the vulnerability, the potential security risks and available work-arounds or mitigations. This confidential stage must have a reasonable duration to enable our customers to take appropriate measures to reduce the impact of the detected flaw on the security and safety of the public.

In the public stage, the security vulnerability will be publicly disclosed and will be included in our â??List of Vulnerabilities.â?• To support the Responsible Disclosure approach, we request reporters of security vulnerabilities to coordinate their disclosure plans (if any) closely with us: ideally our public

disclosures should be simultaneous.

Reporting a Security Vulnerability

In case, the issue is not included in the List of Vulnerabilites, please contact the OpenSynergy Security Team by sending an email to psec@opensynergy.com including the following information:

- Your name, contact information and affiliation (customer, partner, independent research institute,â?¦)
- A description of the vulnerability and the environment in which it was discovered
- Detailed steps to reproduce the vulnerability
- The name, version and configuration details of the affected product
- Any specific plans (e.g. disclosure) or expectations you have around the reported Vulnerability

Date Created
2023/02/09
Author
salmaazmi