CYBSEC S.A.
www.cybsec.com

CYBSEC Security Vulnerability Disclosure Policy

The present policy details CYBSEC procedure regarding the public disclosure of security vulnerabilities. The intention behind this policy is to enable all related parties (i.e. software vendors, researchers and customers) to address the vulnerability in such a way as to mitigate to a minimum any associated risks.

This policy establishes the guidelines followed by the research team upon the discovery of a security vulnerability, it details the steps followed by the research team and the interaction with the software vendor.

The goals of this policy are the following:

- Educate all parties involved, providing the security community with the necessary information to reproduce, study and verify the vulnerability in question.
- Minimize of the risks to all affected parties.
- Contribute in making software more secure.
- Provide the software vendor with the necessary information to release a solution to the vulnerability in question.
- Contribute to research in the security field.

Steps involved in the process of disclosing vulnerabilities

This section outlines the basic steps taken by CYBSEC's research team regarding the disclosure of a security vulnerability. Depending upon the specific situations not all steps may be followed, this depends highly on the vendor's effort to provide a solution and validate the vulnerability.

Below is an enumeration of the different steps with a detailed description of each one in the following section.

1. Discovery: CYBSEC unveils a security vulnerability.
2. Vendor Notification: The vendor is notified of the vulnerability and is aided by the research team with as much technical information as possible.
3. Vendor Corroboration: The vendor should proceed with the reproduction of the vulnerability to verify CYBSEC claims.

4. Fix Development: Once the problem is correctly diagnosed and isolated, the vendor should develop a fix (patch) to the problem in question. The fix may be tested by CYBSEC, prior to release, to ensure the issue is correctly resolved.
5. Advisory Release: The security advisory is publicly released by CYBSEC in a coordinated fashion with the vendor involved. The vendor may then release his own advisory regarding the availability of a fix.

Details of the steps involved in the process of disclosing vulnerabilities

Discovery:

Once the vulnerability has been discovered, it is then studied until it can be fully reproduced. Then an internal document regarding the vulnerability is produced, which includes the following information:

- Description of the vulnerability discovered and the potential risks it imposes.
- Technical information, as in detailed as possible, regarding the steps required to reproduce the vulnerability.
- Proof of concept code, if applicable.

Vendor Notification:

Once the document has been produced, the vendor is contacted (via email or phone, depending on the vendor), and a copy of the internal document is handed to the vendor. This first contact is to be referred as “initial notification date”. The document given to the vendor makes reference to this document.

If the vendor doesn’t provide security related contact information, CYBSEC tries the official contact avenues of the vendor. If none are given, the advisory is made public.

A new attempt to contact the vendor is made, if the vendor hasn’t acknowledged the previous contact, after a 3-day period since the initial notification date.

The advisory will be made public, if the vendor hasn’t acknowledged the previous contact informing that they have read the document and outline a schedule for the resolution of the security issue, after a 7-day period since the initial notification date.

Vendor Corroboration:
This phase is only considered for timing purposes. The details of this phase are on the hand of the vendor. Nevertheless, we give the following suggestions to provide a trustworthy solution to the security problem.

The vendor should follow some variation of the following steps:

- Reproduce the security vulnerability.
- Determine if the vulnerability has already been solved or was already known, in which case CYBSEC should be informed of this situation.
- Determine if any other of the vendor's products (base on the one with the vulnerability or with similar functionality) have the same vulnerability.
- Isolate the code involved.
- Correct the vulnerability.

The vendor should contact CYBSEC, every week during this phase to provide status updates. If this fails to happen, CYBSEC will release the security advisory.

Fix Development:

This phase involves primarily the vendor since during this phase the vendor should address the vulnerability by creating a patch or providing a workaround.

The vendor may request time extensions when necessary, justifying the time required.

The vendor should test the patch prior to release, to ensure that it won't disrupt working installations. The vendor is encouraged ask for CYBSEC collaboration for the testing phase of the developed patch.

The vendor is encouraged to resolve the issue within 30 days of the initial notification date. If CYBSEC considers the need for more time, and feels that the vendor is giving the issue the necessary importance, more time shall be given. If this is not the situation after 45 days of the initial notification date, CYBSEC will make public the advisory.

Advisory Release:

Through cooperation from the vendor, a date for public release of the security advisory will be reached. This date will be set in order to allow for a patch to be made available as soon as the advisory is released. The "release date" will only suffers changes for one of the following motives:

- A third party makes public the vulnerability; therefore CYBSEC will publish the advisory in order to help provide workarounds to the community.
- If the vendor asks for a time extension and CYBSEC considers it has been done in good faith.
- If the vendor can't agree with CYBSEC about a release date, CYBSEC will publish the security advisory after 15 days.

If at the date assigned for release, the vendor hasn't resolved the vulnerability and hasn't contacted CYBSEC, the advisory will be released.

The following information will be contained in the security advisory.

- **Advisory Name:** A name assigned to the vulnerability by CYBSEC:
- **Vulnerability Class:** The type of vulnerability in question.
- **Release Date**
- **Affected Applications:** Vendor's products on which the vulnerability has been detected and successfully tested.
- **Not Affected Applications:** Other versions of the products mentioned before where the vulnerability is not present.
- **Affected Platforms:** Platforms on which the product has been tested positively for the vulnerability.
- **Not Affected Platforms:** Platforms where the product seems unaffected by the vulnerability.
- **Local** / **Remote:** Whether the vulnerability can be exploited remotely or locally.
- **Severity:** Risks imposed by the vulnerability.
- **Author:** Author of the vulnerability.
- **Vendor Status:** Whether the vendor is aware of the vulnerability (i.e. has acknowledged our communications with him), and if a patch is available from the vendor.
- **CVE Candidate:** CVE candidate number.
- **Reference to Vulnerability Disclosure Policy:** Link to this policy.
- **Overview:** Description of the product involved and the vulnerability detected.
- **Vulnerability Description**
- **Technical Details***
- **Solutions:** Possible solutions, including links to vendor information (patch releases, etc.) and workarounds.
- **Vendor Response:** A description of the vendor's response regarding how they dealt with the vulnerability.

* Technical details may not be present. In that case the publication will be catalogued as a *pre-advisory* and an advisory (including technical details) will be published three (3) months later.