



INFIGO IS Disclosure policy

Purpose
Definitions
Process
Policy

June 2008.



Copyright

This document may only be distributed electronically in its entirety through the INFIGO IS web site.

This document may not be modified, edited, amended or reprinted in any medium other than electronically except by INFIGO IS.

Disclaimer

This document is available for informational purposes only. Although reasonable efforts have been made to ensure accuracy of the information contained in this policy, it may include inaccuracies or typographical errors and may be changed or updated without prior notice. Statements presented in this document reflect judgment at the time of publication and are subject to change.

INFIGO IS assumes no responsibility for errors, omissions or damages resulting from the use of information stated in this policy.

Infigo IS d.o.o.
Horvatovac 20
10000 Zagreb

tel. +385 1 4662 700
fax. +385 1 4662 701
info@infigo.hr
www.infigo.hr



1. Purpose

The purpose of this policy is to define how INFIGO IS ("INFIGO", hereafter) manages public reporting of security vulnerability information about products developed by other organizations, maintainers, developers, owners, vendors.

This policy defines a set of rules for interaction between the INFIGO research team and software vendors (or other organizations), when a software security vulnerability has been discovered by the INFIGO research team.

2. Definitions

ISSUE - is a vulnerability, problem, or otherwise a reason for contact and communication.

VENDOR - an individual, group or other organization that supports and maintains software, hardware or other resources that are subject of the ISSUE.

DATE OF CONTACT - point in time when INFIGO contacts the VENDOR.

3. ISSUE disclosure process

The phases of the ISSUE disclosure process are:

1. **Discovery** - INFIGO discovers the ISSUE through casual evaluation, by accident or as a result of a focused analysis and testing processes.
2. **Notification** - INFIGO notifies the VENDOR about the ISSUE. The VENDOR provides INFIGO with the assurances that the notification was received.
3. **Validation** - the VENDOR verifies and validates INFIGO's claims about the ISSUE.
4. **Resolution** - the VENDOR tries to identify where the ISSUE resides and develops a patch or workaround that eliminates or reduces the risk of the vulnerability. The patch is then tested by INFIGO to ensure that the ISSUE has been resolved.
5. **Release** - INFIGO (and optionally, the VENDOR) releases information about the vulnerability, along with its resolution.

4. Policy

The following describes how INFIGO operates during each phase of the ISSUE disclosure process.

4.1. Discovery

In the discovery phase of the ISSUE disclosure process INFIGO will validate the findings and write the ISSUE report. The ISSUE report will include the following information:

- A text-only advisory describing the ISSUE, including affected platforms and versions,
- A detailed technical description of the ISSUE including detailed instructions for reproducing the ISSUE,
- Additionally, if possible, 'proof of concept' code.

4.2. Notification

After the ISSUE has been discovered and researched, INFIGO will send initial e-mail regarding the ISSUE to the VENDOR.

The point in time when the e-mail is sent by INFIGO is considered the DATE OF CONTACT.

INFIGO will make best effort to review all available information regarding the ISSUE or related to the VENDOR for indication of a proper method of contact.

If INFIGO is not able to locate appropriate e-mail address of the VENDOR, INFIGO will send information about the ISSUE to the following e-mail addresses:

- security-alert@[VENDOR],
- secure@[VENDOR],
- security@[VENDOR],
- support@[VENDOR],
- info@[VENDOR],
- secalert@[VENDOR],
- sales@[VENDOR], regardless of their existence.

The initial contact e-mail from INFIGO will inform the VENDOR that the security vulnerability has been found in one or more of the VENDOR's products. Since the premature release of detailed technical information regarding an unresolved vulnerability can be dangerous, no details will be included in the initial contact e-mail. All information should be encrypted, unless the VENDOR cannot support e-mail encryption. INFIGO uses PGP for e-mail encryption.

The initial e-mail sent to the VENDOR will also reference this policy.

The VENDOR is given 10 working days from the DATE OF CONTACT to reply to INFIGO. E-mail auto-responses are not considered as confirmation from the VENDOR. If there is no contact from the VENDOR by the end of 10 working days, INFIGO will attempt to contact the VENDOR again. If there is no confirmation in next 5 working days, INFIGO will disclose the ISSUE.

If the VENDOR contacts INFIGO, INFIGO will send a detailed ISSUE report to the VENDOR. This date will be recorded as the FULL NOTIFICATION DATE.

After the full notification e-mail has been sent, INFIGO will expect the response e-mail from the VENDOR within 7 working days. Response e-mail should contain details about how the VENDOR plans to address the ISSUE.

4.3. Validation

During this phase the VENDOR will attempt to address the ISSUE.

After the VENDOR reproduces the vulnerability (and determines that it is not already known and/or resolved), the VENDOR needs to validate the ISSUE.

Depending on the resources and availability, INFIGO will help the VENDOR with the validation phase when requested.

It is the obligation of the VENDOR to provide status updates to INFIGO every 5 working days or as frequently as both parties agree.

If INFIGO does not receive a status update from the VENDOR in an agreed period of time, INFIGO will release the ISSUE.

The vendor should examine its product to ensure that it is free of other problems that may be similar to the reported ISSUE.

4.4. Resolution

The resolution of the ISSUE involves one or more of the following actions:

- patch creation
- configuration change recommendation
- design change
- workaround

It is the obligation of the VENDOR to provide INFIGO with all known configuration changes or workarounds that address the ISSUE. The VENDOR will optionally provide INFIGO with all patches, so INFIGO can conduct their own verification of the fix.

The VENDOR is required to provide INFIGO with status updates every 5 working days. If INFIGO does not receive a status update from the VENDOR in a period of 5 working days, INFIGO will contact the VENDOR again, asking for the status update. If no status update is received in the following 5 working days, INFIGO will release the ISSUE.

4.5. Release

INFIGO will try to coordinate the time of the release with the VENDOR.

If both parties cannot agree to a coordinated release, INFIGO will disclose only summary information regarding the ISSUE in a period up to 20 days. Summary information will not include details of the vulnerability in order to reduce the likelihood that attackers might exploit the product, based on the disclosed information. After the expiration of the 20 days period, INFIGO will publicly release the full security advisory regarding the ISSUE.