Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Compass Security AG

Vulnerability Disclosure Policy

February 2nd, 2011

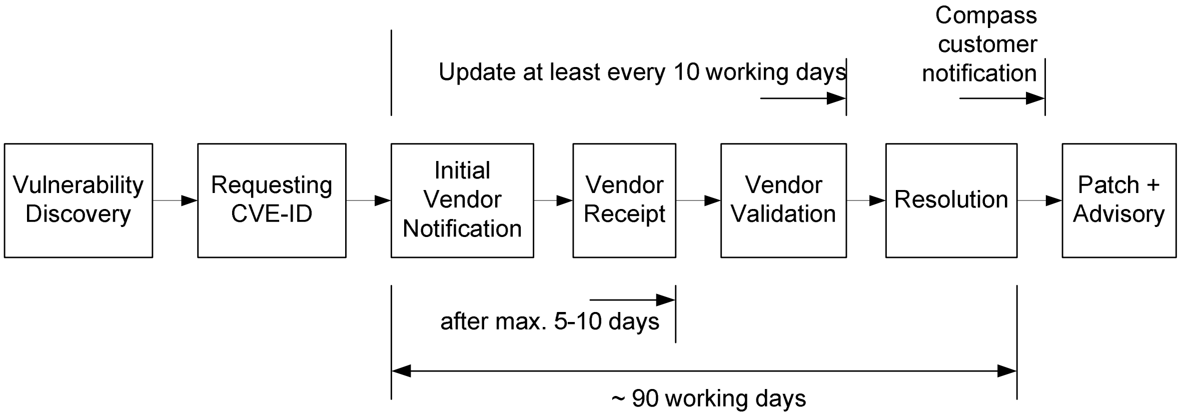
Document Name:	vulnerability_disclosure_policy_english_v3.8.doc
Version:	v3.8
Author(s):	team@csnc.ch, Compass Security AG
References:	-
Date of Delivery:	February 2nd, 2011
Classification:	PUBLIC

Compass Security AG – Vulnerability Disclosure Policy – v3.8

Table of Content

1 Compass Vulnerability Disclosure Process

This checklist is based on the RFC Draft by Steve Christey and Chris Wysopal (see references in chapter 1.8). Compass follows the Vulnerability Disclosure Procedure shown graphically below:



1.1 Full-Disclosure & Ethics

Compass Security AG cooperates with software designers in order to detect vulnerabilities and to eliminate them. The publication of weaknesses without the availability of a suitable correcting measure (patch) is not an aim of Compass. The full disclosure of a weakness is applied by Compass in exceptional cases. See further details in this document.

The protection of customers, particularly those who are in a contractual relationship with Compass, must be guaranteed in any case and Compass will act in the interest of them. Please read through the designed phases of the Compass Vulnerability Disclosure procedure below.

1.2 Vulnerability Discovery

This phase is named "Discovery and description of the weakness". It aims at providing the **vendor** with the essential information for the development of correcting measures.

It must be ensured that the weakness is not known yet and cannot be attributed to a faulty configuration. The weakness is documented in the form of a **PDF**. The facts are described thoroughly with explanations and screenshots, so that the identified weakness can be reproduced, even when the access to the vulnerable system is no longer available.

1.3 Requesting CVE-ID

Next, a CVE-ID from cve.mitre.org is requested for the open weakness. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

1. Email to cve@mitre.org (preferred) or coley@mitre.org
2. Email will contain
   - Affected product, version
   - All identified issues (Categorized by CWE – Common Weaknesses Enumeration)
   - Reason (Compass requires CVE-ID to coordinate with the vendor)
3. MITRE normally responds within 14 days with a CVE-ID per Issue/CWE

Note: MITRE may assign a block of anonymous CVEs to 'frequent releasers' on request

1.4 Initial Vendor Notification

In a first announcement we inform the vendor about the identified vulnerability. Thereby an open and straightforward language should be used. Details of the weakness according to the phase "Vulnerability Disclosure" are provided to the vendor on his request only. Hereby the results must be made anonymous by Compass to avoid any trace back to the Compass customers.

At first Compass tries to identify the security contacts from the Website of the vendor. If unsuccessful, the following mail addresses are tested:

- security-alert@vendor
- security@vendor
- support@vendor
- secure@vendor
- info@vendor

If the above mail contacts are not successful, the contact information is searched via Emergency Centers. (e.g. CERT-CC, SANS Incident Handler).

Finally it is attempted to reach the people in charge of security via the normal contact information of the vendor.

Summarised this means:

- Find security contact via Website
- Guess security contact with mail addresses
- Detect security contact via CERT
- Security Contact via Standard Support of the vendor's Website

If no contact can be identified, Compass Security AG reserves the right to proceed according to chapter 1.10.

1.5 Secure Messaging

In case the contact with the vendor can be established, a safe channel for the exchange of information will be chosen. Generally this means that mails are encrypted using PGP or the use of the Compass Secure Document Exchange solution (www.filebox-solution.com)

1.6 Vendor Receipt

Compass Security assumes that a confirmation by the vendor can be expected within one working week after receipt of the "Initial Vendor Notification". This confirmation means that the vendor has received the information and is now considering further steps.

If the reply message is an automatically generated confirmation, a reply of an individual (human being) should be received within 10 working days (2 weeks).

After a maximum of 10 working days (2 weeks) Compass Security expects a clear feedback from the vendor. If this does not happen, we reckon that we cannot contact the vendor adequately and may continue as described in chapter 1.10.

1.7 Validation

In order to design a patch / workaround the vendor is dependent on detailed information enabling the reproduction of the problem. This information (Source Code, etc.), which has already been gathered in the phase "Vulnerability Discovery", is to be provided to the vendor on request.

Status-updates are expected from the vendor every 10 days. If the contact ceases despite further inquiries, Compass Security reserves the right to proceed as per chapter 1.10.

1.8 Resolution

90 days from the Initial Notification in respect of a real weakness (no false-positive or similar) a patch / workaround or a clear statement of the vendor should be available.

If the vendor delays the publication respectively the development of the fix without any obvious reason, Compass Security reserves the right to proceed as per chapter 1.10.

Compass Security expects an acknowledgement in the Security Advisory provided that the vendor publishes an Advisory.

Example of an acknowledgement by Microsoft for a weakness identified by Compass:

- http://www.microsoft.com/technet/security/Bulletin/MS06-013.mspx

If the vendor is not familiar with the form of Advisories with acknowledgement, Compass Security will publish an Advisory independently (see Advisory Release below).

1.9 Advisory Release

It will be negotiated with the vendor when information about the weakness may be published. This date must be acceptable and realistic for both parties.

The vendor can request a time span of max. 30 days between the publication of the patch and the publication of the Advisory. Within this period no detailed information must be published. This enables the customers to install the patches.

However, Compass Security reserves the right to publish general information, without PoC (Proof of Concept Exploits), beforehand.

1.10 Escalation

In case of problems in respect of this process, Compass Security AG will consider the immediate publication of the weakness on the available distribution channels. (Mailing lists, full disclosure, Compass Website, etc.)

1.11 References

Reference	Link
RFC Cristey / Wysopal	http://www.vulnwatch.org/papers/draft-christey-wysopal-vuln-disclosure-00.txt (expired August 2002)
CERT	http://www.cert.org/kb/vul_disclosure.html
Bruce Schneier	http://www.counterpane.com/crypto-gram-0009.html
Bugtraq	http://www.securityfocus.com/archive/1/description
NTBugtraq	http://www.ntbugtraq.com/default.asp?sid=1&pid=47&aid=48
US Department of Homeland Security	http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf
Marko Laakso	http://www.ee.oulu.fi/research/ouspg/protos/sota/FIRST1999-process/
Rain Forest Puppy	http://www.wiretrip.net/rfp/policy.html
Weld Pond	http://news.zdnet.com/2102-9595_22-523048.html
CVE	http://cve.mitre.org/index.html