



VoIPshield Systems Inc.

Responsible Disclosure Policy

A guide for VoIP vendors on VoIPshield's process of publicly disclosing security vulnerabilities in VoIP products

November 2007



Disclaimer

VoIPshield Systems makes this document available for informational purposes only. It does not represent, warrant or guarantee that it is complete, accurate, or up-to-date, nor does VoIPshield Systems offer any certification or guarantee with respect to any opinions expressed herein or any references provided. This document makes no representations or warranties of any kind and is not intended to constitute legal advice. Readers should not act (or refrain from acting) based on the information herein without obtaining professional advice regarding your particular facts and circumstances. Opinions presented in this document reflect judgment at the time of publication and are subject to change. The information is provided "as is" and VoIPshield Systems assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein.



Contents

Purpose	4
Vulnerability Reporting and Disclosure Process.....	4
Details of Each Stage	5
Stage 1: Discovery	5
Stage 2: Notification and Acknowledgement	6
Stage 3: Investigation, Verification and Validation	7
Stage 4: Release.....	7
Stage 5: Resolution.....	9



Purpose

This policy outlines how VoIPshield Systems (“VoIPshield”) manages the reporting and public disclosure of security vulnerabilities discovered by its research team in products developed by other vendors.

It is intended to minimize the security risk posed by these vulnerabilities by:

- ensuring prompt attention to the verification, validation and resolution of the known issues; and
- alerting users of the affected products to the problems, the potential risks, and the recommended remediation procedures.

Vulnerability Reporting and Disclosure Process

The basic steps of the VoIPshield Vulnerability Reporting and Disclosure Process are described below and are based on “Guidelines for Security Vulnerability Reporting and Response” by the Organization for Internet Safety (<http://www.oisafety.org>).

The vulnerability information VoIPshield provides is supplied as a courtesy to the vendor, and to enhance the security of the user community as a whole.

The process has five stages:

1. **Discovery.** The VoIPshield Security Research Team discovers a security vulnerability either by accident or while working on specific security research.
2. **Notification and Acknowledgement.** VoIPshield notifies the vendor of the vulnerability or vulnerabilities discovered in the vendor’s product(s). This is communicated in the form of a Vulnerability Summary Report (“VSR”). In turn, the vendor provides VoIPshield with acknowledgment that the VSR was received.



3. **Investigation, Verification and Validation.** For each vulnerability, the vendor reproduces and validates VoIPshield's claim(s), and decides on a course of action. This information is communicated to VoIPshield.
4. **Release.** VoIPshield, in concert with the vendor, publicly releases information about the vulnerability, in the form of a VoIP "Security Advisory". The Advisory includes recommendations for temporary remediation and a timetable for permanent resolution.
5. **Resolution.** The vendor develops a patch or workaround that eliminates or reduces the risk associated with the security vulnerability, and makes it available to customers on the schedule communicated in the Security Advisory. VoIPshield will test the vendor's solution to verify that the problem has been corrected.

Details of Each Stage

The following describes the responsibilities of VoIPshield and the vendor during each stage of the Vulnerability Reporting and Disclosure Process.

Stage 1: Discovery

VoIPshield's Security Research Team conducts ongoing research into the security characteristics of products produced by major VoIP systems vendors. Through rigorous testing and results validation this work yields the continual discovery of new security vulnerabilities inadvertently built in to the products by the vendors.

These vulnerabilities are found in both the hardware and software components of the products. They vary widely in type, scope, severity, exploitability, and so on. For whatever reason these design or implementation flaws eluded the testing regimen employed by the vendor, and expose the products and their users to potential security attacks from inside and outside the organization where they are deployed.

With each release of a new product or upgrade, new vulnerabilities are often introduced, making security vulnerability research a perpetual process.



Stage 2: Notification and Acknowledgement

On a schedule determined by VoIPshield, VoIPshield will provide a written Vulnerability Summary Report (VSR) to the vendor showing information on security vulnerabilities discovered in the vendor's product(s) by VoIPshield's Security Research Team.

The VSR will include, for each vulnerability:

- A full description of the vulnerability
- All products and versions in which the vulnerability has been identified
- Configurations used to conduct the research
- Where practicable, step-by-step instructions, proof-of-concept code, or other data that might help the vendor to reproduce the vulnerability.
- VoIPshield's assessment of the severity level of the vulnerability

The vendor will designate an individual or department to be VoIPshield's point of contact for reporting purposes. In the absence of a formal contact, an email will be sent to one or more of the following addresses:

- an appropriate contact as indicated on the vendor's website
- security@vendor.com
- secure@vendor.com
- security-alert@vendor.com
- secalert@vendor.com
- support@vendor.com
- info@vendor.com

VoIPshield will provide a PGP (Pretty Good Privacy) key and request a vendor PGP key before sending the full Vulnerability Summary Report. Upon receipt of the vendor's PGP key, VoIPshield will send an encrypted and signed email containing the VSR.

Once the full notification containing the VSR is sent by VoIPshield, VoIPshield will expect a response by email from the vendor within 7 days that:

- Acknowledges that the vendor has received and read the VoIPshield VSR; and
- Describes the vendor's plans to assess the vulnerability described in the VoIPshield VSR.

In the event that no acknowledgement is received by VoIPshield from the vendor, VoIPshield will attempt to contact the vendor through all known email channels.



All contact attempts throughout the entire process will be documented for potential inclusion in the published Security Advisory under the “Vendor Response” section.

Stage 3: Investigation, Verification and Validation

During this phase it is assumed that the vendor will assess the vulnerability, and determine what course of action it will take to remedy it. VoIPshield will provide reasonable assistance in this process on a best efforts basis. However, the vendor will use its own resources, processes and procedures to examine the vulnerability identified by VoIPshield. These should include:

- The vendor should reproduce the vulnerability. Please notify VoIPshield immediately if this proves difficult and we will assist you.
- Once the vulnerability has been verified the vendor should determine, as soon as it is practicable to do so, but in any case not later than 30 days from acknowledgement of receipt of the VSR, what steps it will take, and on what schedule, to remedy the vulnerability.
- This remedy information should be communicated to VoIPshield so that it can be incorporated into the public announcement of the vulnerability, the formal Security Advisory.
- Under special circumstances, vendors may be granted a “Grace Period” of up to an additional 30 days to make its final communication to VoIPshield of its plans to remediate the vulnerability. This extension will be granted by VoIPshield in its sole discretion, based on the demonstrated efforts made by the vendor during the original 30 day period.

Stage 4: Release

VoIPshield will target to announce the Security Advisory immediately following the 30-days allotted for Stage 3. It is VoIPshield’s strong desire to make this announcement in concert with the vendor.

VoIPshield's Security Advisory will contain (at a minimum) the following information:

a) Advisory Title



- b) Release Date
- c) Severity: A short description of the severity of the vulnerability (e.g. “high”, “medium”, “low”)
- d) Abstract: A brief description of the vulnerability
- e) Products Affected: The names and versions of the vendor’s vulnerable product(s)
- f) Authors: The author or authors of the Security Advisory
- g) Description: A full description of the vulnerability. Contents may include, but not be limited to: a description of how the vulnerability presents itself; configurations that are affected or likely susceptible; potential outcomes of a successful exploit, etc.
- h) Impact: VoIPshield’s opinion of the security implications to the users of the vendor’s system(s)
- i) Recommendations: VoIPshield’s recommendations on available courses of action for customers to mitigate or eliminate the security risk associated with the vulnerability in their environment.
- j) Vendor Response: In this section VoIPshield provides vendors with an opportunity to inform its customers of its plans to temporarily or permanently remedy the security hole in its product(s). VoIPshield anticipates that vendors will want to include items such as: a brief statement of explanation; a link to its own security bulletin; a link to patch information; a planned release date for the patch; other remediation recommendations; etc. It is up to the vendor, in its sole discretion, to provide the content for this section.
- k) Resolution Status: A brief statement to indicate the status of the vendor’s permanent fix for the vulnerability (e.g. “undetermined”; “planned for release on (date)”; “ships with (software upgrade) Version (X.X)”; etc.)

The Security Advisory will not contain the following information:

- Proof of concept code or test code that could readily be turned into an exploit
- Sufficiently detailed technical information that could expedite the writing of exploit code



In cases where VoIPshield has granted the vendor a Grace Period, VoIPshield may include the vulnerability in a “Soft Announcement”, where the existence of the vulnerability will be communicated to the public without disclosing the full details typically included in a Security Advisory.

A Soft Announcement may also be made in the case where another reporter has publicly announced the vulnerability before the scheduled release date of the Security Advisory.

Stage 5: Resolution

The resolution of a vulnerability is the sole responsibility of the vendor. VoIPshield may provide assistance on a best efforts basis. VoIPshield anticipates that these will take one or more of the following forms:

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

The vendor should provide VoIPshield with all information and materials, including the newly created patch if applicable, to allow VoIPshield to test the resolution of the vulnerability.

VoIPshield intends to publish, on a regular basis, the Resolution Status of all announced vulnerabilities.