Security Reporting

If you think you have found a security vulnerability in FreePBX, we would love to work with you to get it resolved!

First Contact

The first thing for you to do is to email **security@sangoma.com**, and **please** include as many details as possible. This includes such things as code snippets and a proof of concept (if you have one). We will evaluate the report and send a non-automated response within 3 (US) business days.

This follow-up may request additional information and require additional time for evaluation if enough detail was not originally supplied. Once verified a private issue will be created visible only to staff and you as the reporter. You will need an account on http://issues.freepbx.org.

Investigation and Resolution

The time this takes will vary greatly based on the amount of detail provided and the ultimate complexity of the issue. The goal is to verify and resolve issues as quickly as possible but there is no guaranteed amount of time. The goal for the entire process is to be at or below Google's Project Zero standard of 60 days, but we expect to be able to work with the CERT standard of 45 days from report to full public disclosure.

Initial Public Disclosure

Once an issue has been verified and fixed an abstract public disclosure will be released. This disclosure will have the following items:

1. Name of component affected
2. Affected versions
3. Fixed versions
4. Credit to the person who discovered the issue (if permitted by the researcher)
5. A CVE if available.

This disclosure will be made via our wiki (http://wiki.freepbx.org), Our Forums (http://community.freepbx.org) and through social media such as http://twitter.com/FreePBX.

Mitigation Period

A minimum mitigation period of 14 days is normally requested to allow the public to act on the information and update as necessary to resolve the reported issue.

Full Disclosure

After the agreed on mitigation period has expired, the reporter may make public full details including proof of concepts and other data to various mediums. Functional details of the exploit will not be released (by us) on our wiki, forums or issue tracker.

Fixed Versions

Current stable, unreleased future versions, and one major release behind will receive security updates.

When possible issues will be fixed as far back as practical, but this may not be practical.

Exploits for older versions may not be fixed. It is recommended that users run on the latest version of FreePBX.

Bounty

Sangoma at its full discretion may compensate reporters of a fully verified vulnerability that has not been previously patched. To be eligible for bounty consideration the reporter MUST follow the guidelines above. The bounty can be paid in Bitcoin (or equivalent crypto-currency) if the security researcher wishes to remain anonymous.