Siren Guidelines

Group Purpose

The purpose of OpenSSF Siren is to encourage public discussion of security flaws, concepts, and practices in the Open Source community with persons that historically are not engaged with or monitoring the traditional upstream communications channels.This would include downstream enterprise operators and organizations managing critical infrastructure. The goal of SIREN is to complement and augment existing channels, such as project blogs and advisories and critical lists such as the oss-security for broader audiences. The members of this group include, but are not limited to, Open Source projects, distributors, security researchers, and developers.

List Membership and Moderation

Membership to this group is not formally restricted but is targeted at Open Source Projects, Distributors, Researchers, Developers, downstream enterprise operators, and organizations managing critical infrastructure..

Anyone can subscribe by and send mail to the mailing list at siren@lists.openssf-vuln.org, regardless of Linux Foundation membership status. New members will have their messages to the mailing list moderated to ensure that the discussions remain on topic and stay positive. Moderators will have to approve messages until the new member is deemed to be a full member. Once a person has shown themselves to be a responsible community member, their messages to the list will no longer be moderated.

Anyone is welcome to subscribe to the mailing list by sending an empty message to siren+subscribe@lists.openssf-vuln.org or signing up here: https://lists.openssf-vuln.org/g/siren. You will be required to confirm your subscription by “replying” to the automated confirmation request that will be sent to you. You will be able to unsubscribe at any time and we will not use your e-mail address for any other purposes or ever share it with a third party. However, if you post to the list, other subscribers may see your address(es) as specified on your message.

A read-only archive of the discussions contained on the list is available to the general public. Additionally, there are social media accounts openssf_siren (X/Twitter) and openssf_siren on Mastodon, infosec.exchange.

List Content Guidelines

- Post to the list should be made in English please

- Be respectful and professional in your messaging. Refrain from personal or organizational hostility. The intention of the list is to share information with defenders, not become an editorial pulpit.
- Plain text mail required (no HTML-only messages)
- When applicable, the message Subject must include the name and version(s) of affected software, and vulnerability type. For example, a Subject saying only “CVE-2099-99999” is not appropriate, whereas “CVE-2099-99999: Acme Placeholder 1.0 buffer overflow” would be OK.
- At least the most essential part of your message (e.g., vulnerability detail and/or exploit) should be directly included in the message itself (and in plain text), rather than only included by reference to an external resource. Posting links to relevant external resources as well is acceptable, but posting only links is not. Your message should remain valuable even with all of the external resources gone.
- This is a security list. Please stick to the topic of security without digressing into other aspects except as it might be necessary to discuss the security aspects in their proper context.
- Please keep discussions relevant to Open Source software. This is not a list to discuss the behavior or problems with closed source software or companies.
- Any security issues that you post to siren should be either already public or to be made public by your posting.
- Security advisories aimed at end-users only are not welcome (e.g., those from a distribution vendor announcing new pre-built packages). There has to be desirable information for others in the Open Source community (e.g., an upstream maintainer may announce a new version of their software with security fixes to be picked up by distributors).
- Occasional announcements of Open Source security tools (and relevant features of non-security tools) are acceptable, but only for initial announcements and major updates (not for minor updates). Especially desirable are news on tools/features aimed to enhance security of other Open Source software.
- Please don't post conference CFPs, (e-)magazine calls for articles, and survey questionnaires. (These are generally cross-posted to lots of places)
- Please don't cross-post messages to siren and other mailing lists at once. If you feel that something needs to be posted to siren and to another list, please make separate postings. You may mention the other posting(s) in your siren posting, and even link to other lists' archives.