SecurityPolicy

Our Security Policy

Reporting a vulnerability

To report a vulnerability you can either email security /at/ spamassassin.apache.org or open a Bugzilla issue being very careful to set the Component to Security so that it is not generally visible. If you create the bug report you will have access to it, as will the security team.

Security team process

The Apache process for vulnerability handling by committers is listed at Vulnerability Handling, which should be read before or along with reading the rest of this page. This writeup is our compatible version, step numbers referring to those in that document.

Once a potential vulnerability is reported to the SpamAssassin committers, the process has satisfied steps 1, 2, and 3.

- If the reporter has opened a Bugzilla issue reporting the vulnerability, ensure that the Component has been set to Security. If the reporter has not already done so, create a new issue with Security component and add the reporter to its Cc list. This will satisfy step 4.
- Determine if this is a valid issue to be fixed and if it should be handled as a security vulnerability. Add comments and change the status of the issue to VERIFIED, CLOSED, change the component if not a security issue, as appropriate. This action with an explanatory comment satisfies steps 5-7.
- If it is a valid new security issue, determine the versions impacted by the issue, and use the comments in the issue to discuss and write up a description of the vulnerability that will allow preparation of a general vulnerability statement explaining the issue.
- Request one or more CVEs, following the instructions in step 8.
- When the ASF security team sends the CVE, follow steps 9 and its related step 11 to begin preparation of the CVE report and announcement text.
- Post discussions of the vulnerability, proposed fixes, drafts of the announcement text, logs of the svn commits, and decisions on a release schedule that contains the fix, all in comments in the Bugzilla issue. The emails sent by Bugzilla will satisfy steps 10, 12, and 13.
- Note that to satisfy step 14, the svn commit message should not mention that it is for a security vulnerability, and also should be worded generally enough that it is not likely to be recognizable as being for this vulnerability even after the public sees the announcement text that is being prepared. Also, unlike non-security issues which are closed in Bugzilla once the fix is committed, leave this issue in Open state until the SpamAssassin release containing the fix is prepared. That prevents people without full access to the issue from matching up the time of closing of the issue with time of svn commit.
- Consider whether there are compelling reasons for early disclosure of the vulnerability to the trusted vendors at mailing-list:distros (*note: read their different addresses for issues that are to be made public within 14 days vs those that will be longer*), or anyone else committers feel like informing. The default steps do not include any early disclosure. However there could be circumstances in which it is deemed important to let vendors incorporate patches for a vulnerability before it becomes public knowledge.
- Prepare a release of SpamAssassin that contains the fix of the issue (step 15).
- Announce the vulnerability as per step 16.
- Note that we skip step 17 which says to edit the svn log to add the CVE identifier to the commit message of the fix. As explained in the above note regarding step 14, we want to obfuscate the connection between the specific commits and the security vulnerability from people who do not already have read access to the Bugzilla issue. Since the process described here results in both the CVE identifier and the commits appearing the issue comments, anyone who does have read access to the issue will be able to find the commits by searching in Bugzilla for the CVE identifier.

Additional guidance may be required. See http://www.apache.org/security/ for more information.