EdgeX Process for Addressing Security Issues

The EdgeX Foundry project takes security threats and issues seriously. In an attempt to address and handle security issues, the EdgeX community (at the hands of the Security WG) will put the following in place for the Edinburgh release:

1. Establish a security mailing address (security@edgexfoundry.org) to allow the user community a means to report security issues to the project with consistency, transparency, and some ease. The emails received by this address should then be redirected to the edgex-tsc-security mailing list for reaction. The security WG, at the direction of the WG chair, will review and respond to the report within one week. See below for response procedures. Note: the archives for edgex-tsc-security mailing list are public, and therefore submissions to security@edgexfoundry.org constitute public disclosure.
2. Establish a security landing page to outline the following (this page should be reachable via the EdgeX Web site home page):
   - How to report a security issue or bug in EdgeX, which will include instructions for emailing the special security email address.
   - Information on expected response time to the report. This response will not necessarily provide a fix, just acknowledgement that the issue has been received and is being worked.
   - A list of known security issues and vulnerabilities – and where possible, correlate the issue against the CVE list. The Common vulnerabilities and exposures (CVE) is a program for identifying, cataloging and addressing software and firmware vulnerabilities. Nationally, the federal government runs the CVE program to help build a free, standardized list or dictionary of security vulnerabilities for organizations to use to improve their software's exposure and posture to security threats. It has been further suggested that this page be prepopulated with already known issues (from known issues, threat assessments and security analysis that have already been completed).
   - A link to the release notes for each release where security vulnerabilities and issues for each release will be highlighted.

Response Procedures

On receipt of a security issue via the mailing address, the Security WG chairman will perform the following:

a. Call a security working group meeting within a week of receipt of the report. At this meeting, work to validate the issue, form an immediate response to the person or organization submitting the report, and notify other members of the community that can help identify and/or fix the issue if the issue is validated.

b. If the issue is validated and deemed critical (see below for levels) by the security working group, inform the TSC chair and form a team to address the issue and possibly release a bug fix as soon as possible.

c. If validated, post the security issue to the security page as a known security issue or vulnerability. Also update the release notes of the effected releases to indicate the same issue.

d. Setup a central security task queue/tracking list (JARA, Kanban etc) so that the issues can be assigned and tracked properly. Some issues will be added by both security as well as individual working group so it is possible an issue may have multiple owners.

Issue Levels

Issues that are high, medium or low will be addressed by the Security Working Group will be addressed as part of the planning for the next EdgeX release.

EdgeX grades security issues on the CVSS (Common Vulnerability Scoring System) scale. The four levels are critical, high, medium and low level issues.