Security

EdgeX Foundry takes security threats and issues seriously.

Reporting A Security Issue

This policy was approved by the TSC on 5/20/2019.

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 small (3-4 member) Security Issue Review (SIR) Team to look at any newly identified security related issue that comes to the project's attention. This team will be made up of the following: the Security WG chairperson, at least one other TSC member, and at least one person from the community with a security and threat assessment background. The SIR Team and the project will address the issue per the Response Process outlined below.
    a. The SIR Team will be chosen each year at the time of the EdgeX TSC voting. [Allowing for this to be by volunteerism, vote, or selection]
    b. The TSC will approve of the SIR Team members.
    c. The Security WG chairperson will appoint replacements in the event that any member cannot complete their year of service.
2. Establish a security mailing address (security-issues@lists.edgexfoundry.org) to allow the user community a means to report security issues to the project. Mail from this address will be automatically forward to the SIR Team. In the future, a public/private key system could be established to encrypt the data in the email to more securely pass the potential vulnerability to the SIR Team.
3. 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.
- A list of known security issues and vulnerabilities – and where possible a Common Vulnerabilities and Exposures (CVE) style report to accompany the issue. 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.
- Prepopulated the security landing page 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, if the reported issue is a publicly disclosed (ie an EdgeX dependency with a CVE) issue, the issue may be discussed during the next security working group meeting, otherwise the SIR Team will perform the following:

1. Call a meeting of the SIR Team as soon as possible. It is desired that this be within a week of receipt of the report, but is based on the availability of the team members.
2. The SIR Team will assess, validate and grade (see grading below) the issue, and make a determination about how to react to the issue. After making the determination, the SIR team will respond to the submitter to acknowledge receipt of the issue and provide some information (as warranted) about the reaction. Reactions include:
    a. Work with the community to fix the issue (in the latest supported and development releases as applicable) as quickly as possible (for critical issues) and issue a dot release (in coordination with the TSC and release manager). Based on the severity and sensitivity of the issue, appropriate teams in the community to fix and document the issue will be involved. Due to the sensitivity of the issue, all work may not appear in the project's task tracking systems (like GitHub issues) while the issue is being addressed.
    b. Determine that the issue should be fixed in a future release. Document the problem in an issue and assign the work to the appropriate work group chairman for prioritization.
    c. Assess that the issue is of low probability or impact to the project and its user community and decide to take no action other than report.
3. Create a Common vulnerabilities and exposures (CVE) style report of the issue and associated threat.

   See EdgeX+Security+Issue+Template

   Towards defining the fields in this template we examined RSA's vulnerability disclosures and that of

   OpenStack https://security.openstack.org/ossa/OSSA-2019-006.html

4. At a time to be determined by the SIR Team (based on the sensitivity of the issue and potential time to fix), the SIR Team will:

    1. Post the CVE report to the edgex-tsc-security mailing list. Note: the archives for edgex-tsc-security mailing list are public, and therefore submissions to security@edgexfoundry.org constitute public disclosure.
    2. Post the issue and CVE report to the above-mentioned security landing page as a known security issue or vulnerability. All issues captured in EdgeX Wiki.
    3. Advertise release specific patch sets to address the issue (with link).
    4. Major issues will be reviewed & discussed during weekly security working group meeting.

As a side note, when an issue is created in GitHub, the issue should carry a "security_audit" label so as to highlight the work as it relates to this process.

3rd Party Dependency Security Issues

When a CVE (or other security issue) is reported on an EdgeX dependency (code or library not managed and maintained by the EdgeX community) that issue will trigger the same response procedure. The only difference in the process is that the EdgeX community will defer to the owning community for fixes.

The SIR team should periodically monitor the security issues and vulnerabilities pages of the third party dependencies and trigger the response procedures accordingly when a new issue has been discovered that has not yet been handled in EdgeX.

As for now, SIR team is relying on two products to scan and detect security vulnerabilities largely, which are Snyk and Clair scan. Once an issue is found, the SIR team will follow steps mentioned in "Response Procedures" accordingly.

Issue Levels

Issues that are deemed **high**, **medium** or **low** 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.

SIR Team Member Qualifications

The SIR team member brings security knowledge, product experience to comprehend issue ramifications, has contributed to one or more EdgeX components, passion, and a can-do attitude. She/he must honour the requirement to responsibly disclose (see responsible_disclosure) security issues. In essence not disclose the issue to the public all a fix or workaround is developed and we have had an opportunity to alert known production deployments to apply the fix. The SIR team member will aid in triaging the issue (develop clear understanding, rank it, assist and/or identify EdgeXers to help develop fix or workaround and document the issue). The SIR team will work with QA and product roadmap teams to test fixes, determine release timeline respectively.

Release Specific Known Issues