

Istio Product Security Working Group

What it is and Why it's Important

Brian Avery / Red Hat / @briansvgs
Jacob Delgado / Aspen Mesh



#IstioCon

What is the product security work group?

Created with the goal of **resolving**, **identifying**, and **preventing vulnerabilities** in Istio by:

- Addressing vulnerability disclosure reports and transparently informing our community and users.
- Providing new security guidelines in Istio's development lifecycle.
- Establishing the security threats of Istio as a product: dependencies, add-ons, and antipatterns in order to recommend the best security practice to our developers and users.

Charter:

<https://docs.google.com/document/d/1nKamSxTlnU1CWmPxc5MxKKTr7o8Y5OAez8DOvwddUyA>

#IstioCon



A brief history

- Product Security *Committee* handled CVE fixes
 - This was a smaller group of people
 - The process wasn't formalized making coordination difficult at times for the many tasks required to publish a CVE
- Product security working group created in March 2020 to enable this process coordination



Who is on the Product Security WG

- TOC representation
 - Josh Blatt (Google)
 - Neeraj Poddar (Aspen Mesh)
- 15 people are in the Product Security WG
- Many companies are represented (alphabetical order)
 - Aspen Mesh
 - Google
 - IBM
 - Invitae
 - Red Hat



Product Security vs Security Work Group

Product Security

- Security of Istio itself
 - Fixing vulnerabilities
 - Preventing new issues

How can we keep Istio, as a product, secure?

Security

- Istio Security Features
 - Authentication
 - Authorization
 - Certificate management
 - Etc

How can features in Istio be used to secure environments?



Vulnerability Scoring

#IstioCon



Our goals in addressing a report

When a report is received, the Product Security WG is responsible for triaging and assessing the report.

- Can we reproduce it?
- How easy is it to exploit?
- Is control plane exploitable?
- Is data plane exploitable?



What is a CVSS score?

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. This is a score from 0-10 based on:

- *Confidentiality*
- *Availability*
- *Integrity*
- *How easy it is to exploit*

How does it affect the user's environment? It's a formula, not a science.

As the score goes up it is easier to exploit.



How we address CVSS scores

| Score | How it is fixed | Importance to end user |
|-----------------------------|-------------------------|-----------------------------------------|
| Less than 6 | Fix in public | Generally low concern |
| Greater than 6, less than 7 | Considered case by case | Consider importance to your environment |
| Greater than 7 | Fixed in private | Suggest upgrading as soon as possible |

Alpha features, while not technically supported, are evaluated on a case by case basis.

<https://istio.io/latest/about/feature-stages/>

#IstioCon




Looking at 2020

- 11 security bulletins
 - Source: <https://istio.io/latest/news/security/>
- 17 CVEs
 - By Score
 - < 6: 3
 - 6-7: 2
 - >7: 11
 - 1 does not have a score

Istio versions still receiving security updates:

- 1.9
- 1.8



Only Istio
1.8 and 1.9
are
currently
supported



Security Bulletins

<https://istio.io/latest/news/security/>

| Disclosure | Date | Affected Releases | Impact Score | Related |
|-----------------------------------------|--------------------|-----------------------------------------------------------|--------------|-------------------------------------------------------------------------------------------------------------------------------|
| ISTIO-SECURITY-2020-011 | November 21, 2020 | 1.8.0 | N/A | Envoy incorrectly restores the proxy protocol downstream address for non-HTTP connections |
| ISTIO-SECURITY-2020-010 | September 29, 2020 | 1.6 to 1.6.10 1.7 to 1.7.2 | 8.3 | |
| ISTIO-SECURITY-2020-009 | August 11, 2020 | 1.5 to 1.5.8 1.6 to 1.6.7 | 6.8 | Incorrect Envoy configuration for wildcard suffixes used for Principals/Namespaces in Authorization Policies for TCP Services |
| ISTIO-SECURITY-2020-008 | July 9, 2020 | 1.5 to 1.5.7 1.6 to 1.6.4 All releases prior to 1.5 | 6.6 | Incorrect validation of wildcard DNS Subject Alternative Names |
| ISTIO-SECURITY-2020-007 | June 30, 2020 | 1.5 to 1.5.6 1.6 to 1.6.3 | 7.5 | Multiple denial of service vulnerabilities in Envoy |
| ISTIO-SECURITY-2020-006 | June 11, 2020 | 1.4 to 1.4.9 1.5 to 1.5.4 1.6 to 1.6.1 | 7.5 | Denial of service in the HTTP2 library used by Envoy |
| ISTIO-SECURITY-2020-005 | May 12, 2020 | 1.4 to 1.4.8 1.5 to 1.5.3 | 7.5 | Denial of service affecting telemetry v2 |
| ISTIO-SECURITY-2020-004 | March 25, 2020 | 1.4 to 1.4.6 1.5 | 8.7 | Default Kiali security configuration allows full control of mesh |
| ISTIO-SECURITY-2020-003 | March 3, 2020 | 1.4 to 1.4.5 | 7.5 | Two uncontrolled resource consumption and two incorrect access control vulnerabilities in Envoy |
| ISTIO-SECURITY-2020-001 | February 11, 2020 | 1.3 to 1.3.7 1.4 to 1.4.3 | 9.0 | Authentication Policy bypass |

#IstioCon



Timely Response to Vulnerability Reports

Goal: Respond to all vulnerability reports within 30 days

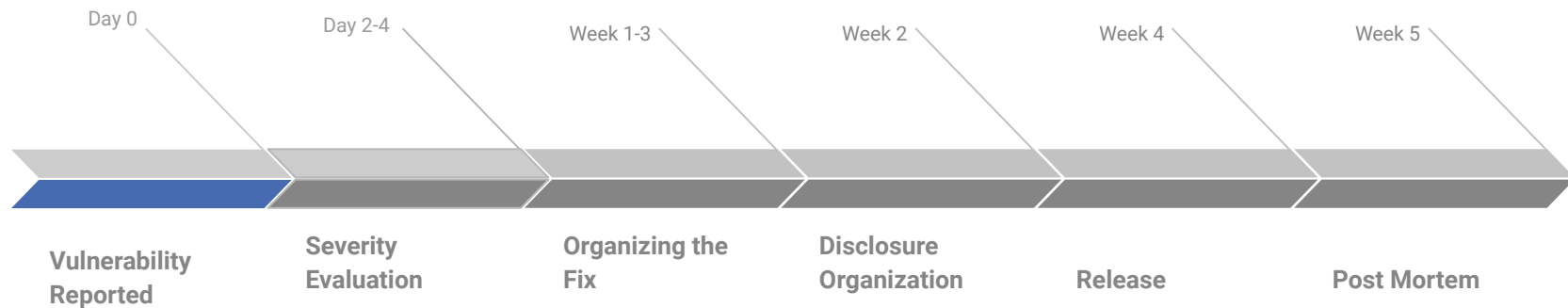


Incident Command System

- Using a proven, reliable method for attacking vulnerabilities ***in a timely manner*** is vital to the success of Istio and the Product Security WG
- The Incident Command System is the model the Product Security WG uses to formalize fixing vulnerabilities.
- Coordinating this effort is ***difficult***
 - Release Managers/Working groups/Subject matter experts
 - Messaging concerned audiences
 - Building/Testing/Publishing



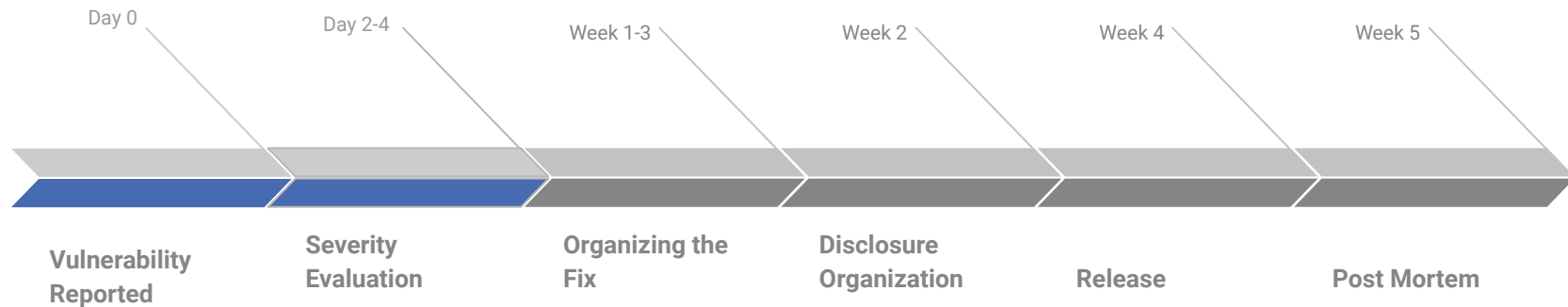
A Vulnerability is Reported



Product security workgroup acknowledges to the reporter that their report has been received and an assessment will take place within the next 72 hours.



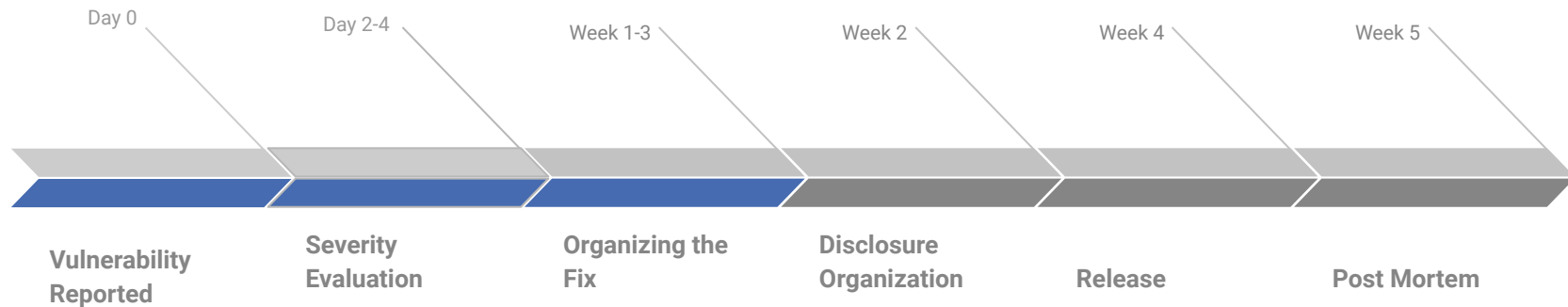
Severity Evaluation



A CVSS score is created by a member of the team. The rest of the team is tasked with reviewing the score. Depending on the score, a fix lead is assigned to organize the fix.



Organizing the Fix

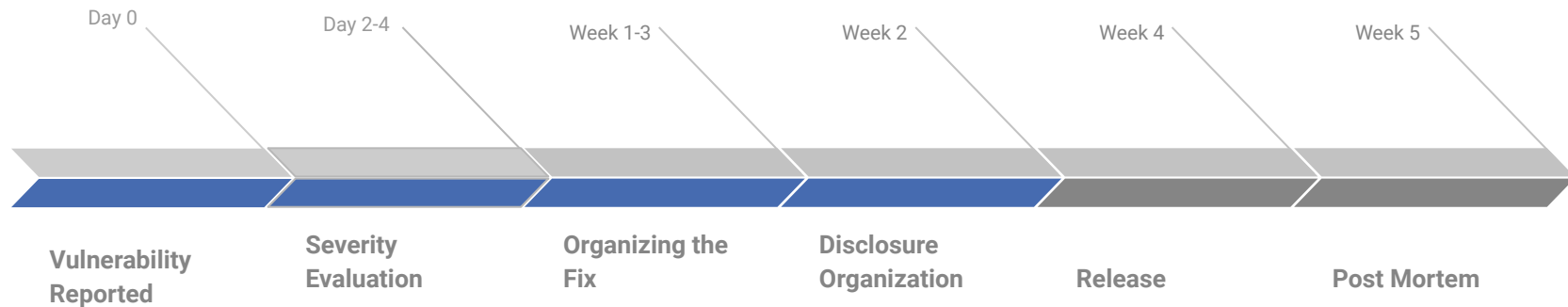


The fix lead is responsible for:

- Finding SMEs capable of fixing the issue
- Aligning embargoes with 3rd parties and dependencies, if necessary
- Finding a test lead to validate the vulnerability and fix
- Finding a communication lead that will prepare release notes, email the early disclosure list, post on discuss, etc...



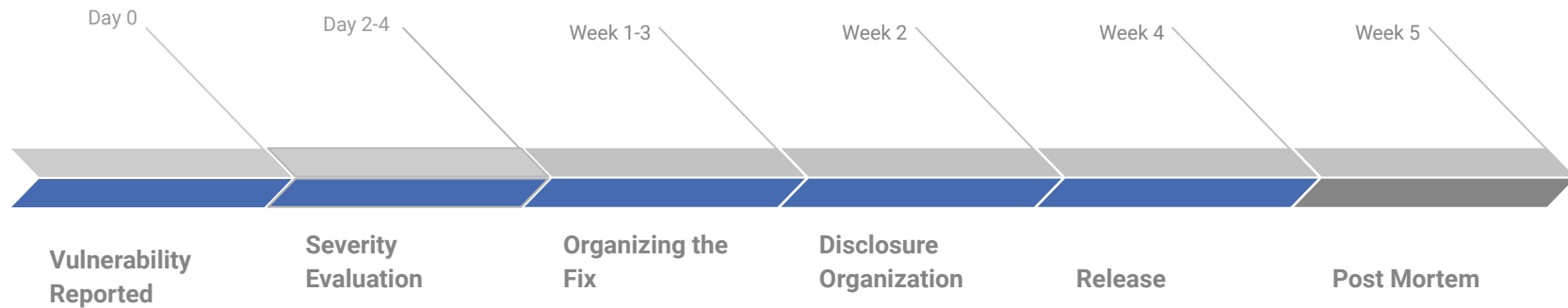
Disclosure Organization



- The Istio Early Disclosure list is notified of a pending release along with other details.
- An announcement is made notifying our users of a pending CVE patch within 2 weeks



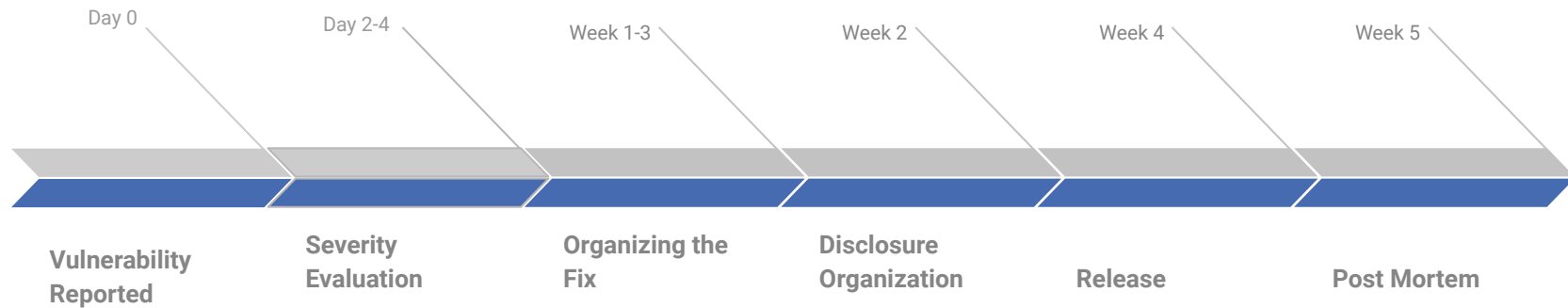
Release



- The appropriate versions have been built
- Qualification/Performance tests have been run, similar to that of other patch releases
- Posted to istio.io
- Disclosure of CVE



Post Mortem



Product Security WG meets to discuss process improvements and other details to improve upon for the next CVE.



Making Istio Security Transparent

#IstioCon



Making Istio Product Security Transparent

- Reporting Istio fixes in multiple places, in advance and upon release
- Central page to view a list of vulnerabilities
 - Updates to <https://istio.io/latest/news/security/> coming soon
- Public post mortems
 - <https://tinyurl.com/pswgdrive>
 - Will update soon with some of our previous disclosures
- Istio community product security meeting
 - tinyurl.com/istioWorkgroups

Join us for our next monthly meeting on March 3rd at 12pm EST

#IstioCon



Proactive Measures

#IstioCon



Image Vulnerability Scanning

- Examines packages installed in an image for known vulnerabilities
- We scan docker images using IBM's scanner before release
- Istio does not do rolling releases.
 - We make sure that our image scanner reports no vulnerabilities before release. Older images may report dependency vulnerabilities over time. These are fixed in newer releases.



Proactive Measures: Where Are We?

- 3rd Party (NCC) Audit of Istio code
 - Results were reviewed during some of our open meetings
- Working relationship with the Envoy Security team
 - 2/3rds of CVEs in 2020 were found in Envoy
 - They responsibly disclose issues with us
 - We may have a difference in opinion on score
 - Issues are sometimes reported to us that we report to Envoy
- Tighter integration with other dependencies



Guide to secure your service mesh

- Guide to deploying a secure Istio environment based on recommended practices
 - <https://istio.io/latest/docs/ops/best-practices/security/>
 - New as of Feb 18th
- Some of the suggestions
 - Enable mTLS in STRICT mode
 - Use of Authorization policies
 - Disable automatic protocol detection

We recommend you thoroughly read and understand the contents of the guide



2021 Roadmap

#IstioCon



Dependency Scanning

- Scan for outdated code dependencies
- For example, outdated versions of Go
- Coming soon



Code Scanning

- Scan for common patterns to catch vulnerabilities before code is merged
- For example, using user input before validation
- Coming soon



Istio Threat Model

- Threat modeling is a structured process to identify and enumerate potential threats such as vulnerabilities or lack of defense mechanisms and prioritize security mitigations.
- CVSS and Kubernetes scoring system help us prioritize and evaluate vulnerabilities, but they are vague and need to be taken in a different context than they were built for.
- A threat model built for Istio will help us evaluate and prioritize vulnerabilities specifically within the context of Istio.
- Envoy already has developed its own:
https://www.envoyproxy.io/docs/envoy/latest/intro/arch_overview/security/threat_model



Stay informed

#IstioCon



How can you stay up to date?

- Are you a partner? Please join our early disclosure list. More information here:
 - <https://tinyurl.com/istioearlydisclosure>
- We post release announcements on
 - RSS: <https://istio.io/latest/news/feed.xml>
 - Discuss: <https://discuss.istio.io/>
 - Twitter: <https://twitter.com/IstioMesh>
 - Slack: #announcements
 - Google Group coming soon!
- Sorry, but we do not have a public slack channel in order to encourage responsible disclosure
 - Do not product security issues to #security



Where do you expect to find information about security releases?

Please answer in the Istio Slack
#istiocon

#IstioCon



How Can You Get Involved?

- Join us in our monthly community meetings. The next one is March 3rd at 12pm EST
 - <https://meet.google.com/vao-otzc-hvx>
- Help us find and privately report vulnerabilities

Email *istio-security-vulnerability-reports@googlegroups.com*

Do not write github issues!



What to do if I have a concern

- If you **experience** a crash with the control plane or data plane
- You *think* you discovered a potential security vulnerability in Istio
- You are *unsure* how a vulnerability affects Istio
- You *think* you discovered a vulnerability in another project that Istio depends on
- If you aren't sure if an issue is related to Envoy or Istio, we're happy to help point you in the right direction

Email **istio-security-vulnerability-reports@googlegroups.com**
It is better to err on the side of caution than it is write a GitHub issue or post publicly.



Questions?

#IstioCon



Thank you!

Brian Avery / twitter: @briansvgs / Red Hat Senior Software Engineer

Jacob Delgado / Aspen Mesh Principal Software Engineer

#IstioCon

