Product Security Incident Response Plan (Version 1.1)

1 Introduction

Our Product Security team guides our product teams in building our solutions backed by secure development practices and industry standards. The final phase of secure development focuses on incident response and the necessary steps *the Company* must take to remediate and prevent vulnerabilities in our Products and supported Services (Offerings). As vulnerabilities are publicly posted, disclosed and identified, *the Company* quickly assesses and remediates these vulnerabilities to ensure our products are secure for our customers, their platforms and ecosystems.

The charter for the *Company's* Product Security team states *the Company* will manage security of the deliverables to customers and the [open source] community. To meet this, *the Company* Product Security's Incident Response is established to act as executive agent in coordinating vulnerability response across all of *the Company's* products and corporate teams herein named the Product Security Incident Response Plan (IRP).

The Company Product Security IRP proactively prepares *the Company* and Product Security to effectively handle security incidents related to Offerings produced by *the Company* through four phases:

1. Notification & Triage
2. Assessment & Coordination
3. Remediation & Release
4. Recovery & Close

The Company's Product Security team can properly manage security issues in a timely manner as they relate to *the Company's* Offerings by following these four phases. This process allows for successful delivery and timely information to our customers, partners, and other stakeholders. The IRP details the "what, where, who, why, and how" of *the Company's* incident response - irrespective of the severity of the security vulnerability.

1.1 Objective

The Company's Product Security Incident Response process uses a [centralized hybrid] model involving multiple teams and roles within the Secure Engineering Team, the Product Security organization, and the larger Engineering organization. This document sets the expectations for all teams or associates across *the Company* who participate in the incident response process. The roles, referenced processes, and procedures contained in this document are structured to articulate the overall incident orchestration, the different workflows during each incident, and the expected actions for each responsible team or associate.

1.2 Incident Response Plan Scope

The Company's Product Security IRP outlines the orchestration process *the Company* uses to coordinate a response to all security vulnerabilities reported or discovered within *the Company's* offerings. This plan establishes the baseline on which *the Company* classifies the level of severity for vulnerabilities, which drives the risk to *the Company* offerings, its customers, and the overall ecosystem and therefore drives the

orchestration of efforts necessary to respond to incidents.

The IRP establishes communication and coordination between stakeholders, providing a high-level process on how *the Company* responds to incidents from inception until closure, including follow through with a retrospective review of the event for potential enhancement or modification of this plan.

Additionally, the IRP defines key terminology, deliverables, and identifies the stakeholders, both involved in the process, and those that need to be informed of the outcomes/deliverables of the process. Thus, the base plan is not meant to be a detailed checklist of all tasks performed during incident response, but simply an overview of the processes set in place to adequately triage, remediate and release a fix for a vulnerability.

Supporting procedures are linked throughout the IRP and establish the workflows and checklists to support the actions taken in the IRP.

This IRP will be reviewed and updated at least annually. Incremental changes can also occur as a result of incident retrospective improvements. Changes or amendments to the plan require approval from the Product Security Director and communicated to all stakeholders as appropriate.

1.3 Incident Response Plan Overview

The Company's Incident Response process flow is broken up into four phases:

1. Notification & Triage
2. Assessment & Coordination
3. Remediation & Release
4. Recovery & Closure

A successful incident response effort begins with the notification and triage/validation of a problem and continues with the orchestration of stakeholders to adequately respond to and remediate an issue. This process allows for open communication of that knowledge to the stakeholders / community.

Figure 1

1.3.1 Notification & Triage

The Notification & Triage phase focuses on the intake and initial triage of the task. This initial triage process determines any effects on *the Company's* components and offerings, assigning a unique Common Vulnerability and Exposures (CVE) number to each vulnerability, establishing an internal Common Vulnerability Scoring System (CVSS) score, identifying the vulnerability type/family through the Common Weakness Enumeration (CWE) classification, assigning a severity rating to each product affected by the CVE for passing to Product Engineering. These triage and scores will be published on *the Company* CVE pages immediately after triage from disclosed or coordinated vulnerabilities unless they are under an embargo.

1.3.2 Assessment & Coordination

The Incident Response continues with a formal assessment of the vulnerability. This process includes the validation of the vulnerability, confirming *the Company's* severity level, and identifying possible mitigations/remediations.

During this formal assessment, Incident Response analysts initiate the drafting of the documentation providing a technical explanation of the vulnerability and forming potential remediation options. After Incident Response completes a full assessment, the Product Engineering organization is officially informed about the vulnerability affecting their products via a tracker filed in their issue tracking system, containing the relevant information pertaining to the product. Product Engineering then verifies the information for the offerings affected, collaborates on the documentation of the vulnerability for their offerings and provides additional guidance as

necessary for a development plan remediating the vulnerability.

1.3.3 Remediation & Release

Secure Engineering drives *the Company's* remediation efforts by orchestrating the overall vulnerability remediation timelines and ensuring they align with the appropriate SLAs for all key stakeholders involved. Product Engineering organization determines the proper remediation for the vulnerability and ensures the documentation of appropriate controls to mitigate the risk of the vulnerability. The Quality Engineering organization tests the remediation and ensures the proposed fix appropriately remediates the vulnerability without introducing any regressions into the code. Release prepares the final build of the code for public consumption.

Additionally, internal control organizations, such Communications, Legal and/or others will collaborate on internal and external communication that supports and accompanies the remediation release for the vulnerability.

1.3.4 Recovery & Closure

The Incident Response organization then concludes the incident response efforts, which involves ensuring final tracking of the incident, internal and external communications are properly developed, reviewed and released, and follow-up activities are completed.

Additional tasks are necessary for an embargoed incident, including embargo disclosure and coordination, public release, fix updates and issue closeout. This final phase will include the retrospective review(s), final public document updates, post-event release of data to public data feeds such as National Vulnerability Database (NVD), CVE, Open Vulnerability and Assessment Language (OVAL) and others, errata release and finally, post event improvements for Product Security or Product Engineering.

2 Key Productization Stakeholders

This IRP exists to support *the Company* in orchestrating a response quickly and uniformly in providing transparency to the ecosystems on our *Open Source* offerings on the handling of security vulnerabilities and incidents. The following shortlist of internal stakeholders includes the teams which are key to the notification & triage, assessment & coordination, remediation & release, recovery & closure, and overall orchestration of an incident. Additional internal stakeholders and *the Company's* external stakeholders are included in the Stakeholder Expectations and Communication Methods section below.

3 Definitions and Outcomes

3.1 Incident Response Process-Specific Definitions

The following key terms are used throughout the Incident Response Plan. Additional terms can be found in the Product Security Glossary.

Term	**Definition**
Flaw	An internal representation of a weakness or vulnerability within the IR workflow, containing all the metadata necessary to describe the issue and create trackers for remediation, as well as security artifacts such as errata descriptions and CVE pages.
Major incident	An issue that has the potential to significantly impact *the Company's* offerings. This includes one or more of the following: 1. Critical, important, or moderate severity ratings 2. Significant potential impact to customer systems 3. May have ease of exploitation by threat actors 4. Have heightened awareness by external stakeholders and/or 5. A higher risk to the ecosystem Major incidents follow a formal declaration and require an orchestrated response across the organization.
Minor incident	An issue that has a lower level of impact on the customer system and is not widely publicized. It imposes a lower level of risk and does not require full orchestration but does require tracking.
Orchestration	Orchestration is the internal and external coordination and communication between stakeholder responses to inform customers, users, and the ecosystem of issues. Orchestration addresses the risk, vulnerability response and/or mitigation efforts to protect the customer and *the Company*.
Task	A "unit of work" analyzed during Incident Response Formal Assessment, indicating that a weakness or vulnerability triaged during Initial Triage needs further assessment and work. Tasks are tracked in the Incident Response Tracking Tool, depending on the offerings, by the appropriate analysts and are only viewable by Product Security.
Vulnerability	An imperfection or absence of a safeguard in an asset that provides a higher potential or frequency of a threat occurring. Vulnerabilities impacting *the Company's* offerings result in a CVE

	assignment, if one is not already assigned by a more specific CNA (CVE Numbering Authority).
Weakness	A fault, bug, or other error in software or hardware implementation, code, design, configuration or architecture that if left unaddressed could result in systems, networks, or hardware being vulnerable to attack. These are addressed with hardening of the system and tracked as a non-security bug defect or improvement to the system.
Security bulletin - SB	In the event of a Major Incident, Incident Response, in collaboration with IR Analysts, Incident Manager and Engineering specialists will create a public-facing document called a *Company* Security Bulletin (CSB) in our Customer Portal, aiming to provide extra information to the community around the vulnerability that was declared as a Major Incident.
Security Advisory - SA	*The Company's* Security Advisories (SAs) are product erratas containing Security Fixes. The product teams are obliged to file SAs when shipping CVE fixes, and Incident Response is responsible for approving the SAs for release in a timely fashion. SA approval by the ProdSec specialist also automatically lifts embargoes.

3.2 CVE

The MITRE corporation is the secretariat for the Common Vulnerabilities and Exposures (CVE) list. CVE is a list of records that identifies and categorizes vulnerabilities in software, firmware, and hardware. Each record includes an ID (ex. CVE-2021-3156), a description, and a public reference for publicly known cybersecurity vulnerabilities. CVEs are an industry standard that provides a common means of identifying vulnerabilities for all concerned.

The Company's Product Security might be a designated CVE Numbering Authority (CNA) for *the Company* portfolio (products / services), being responsible as the authoritative source for assigning CVE IDs within our scope and supplying the description and references to MITRE to populate the records within the CVE list. The CVE list feeds the NIST National Vulnerability Database.

3.3 CVSS Score

NIST's National Vulnerability Database (NVD) will independently assess a given CVE and provide a Common Vulnerability Scoring System (CVSS) score based on the Forum of Incident Response and Security Teams (FIRST) CVSS score calculator (currently version 3.1). *The Company* is an active member of the FIRST CVSS SIG, contributing to the CVSS Standard. *The Company's* Incident Response uses this standard to calculate its own CVSS score for each vulnerability. The CVSS score is a quantitative description used as general guidance for assigning the impact and corresponding *Company* severity level.

3.3.1 CVSS Rescore

For open-source software shipped by multiple vendors, the CVSS base scores may vary for each vendor's version, depending on the version they ship, how they ship it, the platform, and even how the software is configured and compiled. These variations make scoring vulnerabilities difficult for third-party vulnerability databases, such as NVD, which gives a single CVSS base score to each vulnerability.

How the source code was compiled or hardened technologies used can reduce the security severity of a vulnerability. Standalone software may suffer from a vulnerability, but its use within a product may preclude the vulnerable code from ever being used in a way that could be exploited. These differences can cause the scores to vary widely.

For example, NVD may rate a flaw in a particular service as having a high impact on the CVSS CIA Triad

(Confidentiality, Integrity, Availability), where the service in question is typically run as the root user with full privileges on a system. However, in *the Company* products, the service may be specifically configured to run as a dedicated non-privileged user running entirely in an SELinux sandbox, greatly reducing the immediate impact from compromise, resulting in a reduced impact.

If *the Company* determines that the base CVSS score provided by NVD and FIRST does not adequately describe the effect of the vulnerability within *the Company's* offerings, *the Company* will perform a CVSS rescore to accurately reflect the risk of the vulnerability in our offerings. CVSS rescore can happen at any time with a public CVE, but is often initiated during the triage's formal assessment phase.

If there is a significant discrepancy in the CVSS score provided by *the Company* and NVD, *the Company* tooling will detect and flag the vulnerability, noting the discrepancy for resolution. Product Security analysts then conduct a review. This review process results in one or more of the three outcomes:

1. Incident Response adjusts *the Company's* score based on NVD's score.
2. Incident Response provides a statement clarifying why our score differs from NVD.
3. Incident Response submits a request to NVD, asking them to evaluate their score based upon *the Company's* input on the CVE.

The majority of the time, *the Company* will provide a statement clarifying our score differences while at the same time submitting a request to NVD to reevaluate their score.

3.4 *The Company's* Security Vulnerability Severity Rating

After the CVSS scoring is completed, *the Company's* Product Security provides an assessment based on the qualitative four-point scale (Low, Moderate, Important, Critical) defining the appropriate severity. This occurs after a thorough analysis of the vulnerability, assessment of the offerings affected, and risk to the *Company* offerings.

Severity rating	**Description**
Critical impact	This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. Flaws that require authentication, local or physical access to a system, or an unlikely configuration are not classified as Critical impact. These are the types of vulnerabilities that can be exploited by worms.
Important impact	This rating is given to flaws that can easily compromise the confidentiality, integrity or availability of resources. These are the types of vulnerabilities that allow local or authenticated users to gain additional privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication or other controls, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service.
Moderate impact	This rating is given to flaws that may be more difficult to exploit but could still lead to some compromise of the confidentiality, integrity or availability of resources under certain circumstances. These are the types of vulnerabilities that could have had a Critical or Important impact but are less easily exploited based on a technical evaluation of the flaw, and/or affect unlikely configurations.
Low impact	This rating is given to all other issues that may have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences. This includes flaws that are present in a program's source code but to which no current or theoretically possible, but unproven, exploitation vectors exist or were found during the

	technical analysis of the flaw.

3.5 Common Weakness Enumeration

In addition to the CVE, the MITRE Corporation manages the Common Weakness Enumeration (CWE) list. CWE is a community-developed list of software and hardware weakness types. The CWE list and associated classification taxonomy serve as a language used to identify and describe these weaknesses in terms of CWEs, which may, in turn, change development practices.

The Company's Incident Response analysts will analyze vulnerabilities and determine which weaknesses are inherent to the makeup of the vulnerability. CWE information will be collected and stored with the vulnerability for further analysis.

3.6 Embargoes

To 'embargo' a vulnerability is to not publicly disclose the vulnerability and limit the information around it to key stakeholders who need to know and can assist with the security process. Embargoes can help with the security process by giving the software creator and distributors time to research, triage, fully understand, fix, test, and prepare to distribute a software fix or updated version of the affected software, as well as propose workarounds and other mitigations.

A vulnerability is either embargoed or public:

- An embargoed vulnerability is kept private (the fix, security information and typically, the very existence of the vulnerability) until the "Coordinated Release Disclosure" date. While under embargo, access to any information about the vulnerability is limited to relevant members of Incident Response, Secure Engineering leadership, Product Security management, and relevant subsets of Product Engineering and Product Management on a need-to-know basis.
- A public vulnerability is a vulnerability in the public domain; where general information about the vulnerability, its impact, upstream fix, affected status, and mitigation advice of code used by *the Company's* products is available to the public.

A vulnerability is typically embargoed upstream and/or by finders when the vulnerability is discovered. *The Company's* Product Security Incident Response will advise on reasonableness of embargo and preferred timeline, but control lies with the finder or upstream. While most embargoes have either an important or critical severity, depending on the vulnerability, a moderate or low severity vulnerability could be embargoed, but this should be avoided. If there is any public information about the vulnerability, even if it is obscured, then the flaw is not eligible for the embargo workflow.

Only official Company communication tools approved by *the Company's* Information Security and then approved by Product Security should be used to store or discuss embargoed information.

4 Product Security Incident Overview

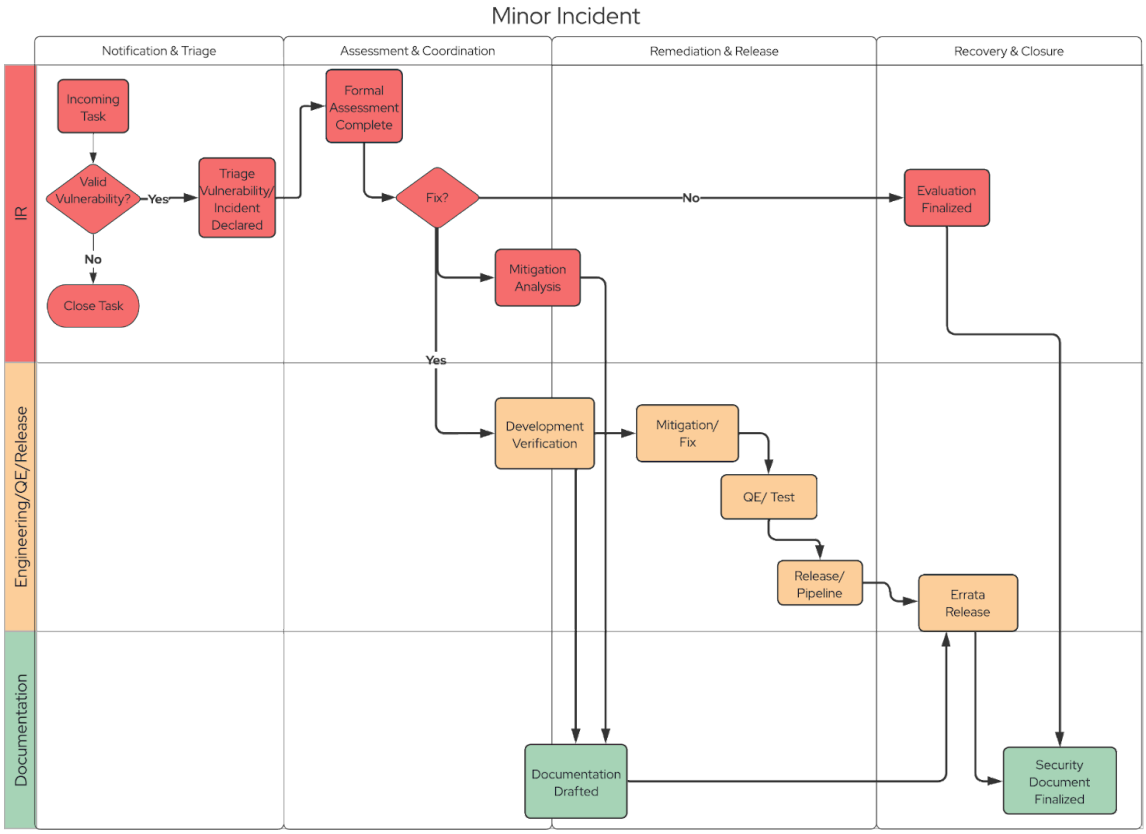
An incident is declared when a new vulnerability affecting a *Company* offering is discovered and validated. Actions are taken to properly assess and remediate the vulnerability or, at a minimum, respond to the vulnerability publicly. All vulnerabilities are triaged, mapped to a *Company* severity level, and then declared as either a major incident or a minor incident. This declaration outlines the level of orchestration throughout the Product Security and into the *Company* organization in handling the incident.

4.1 Minor Incidents

Minor incidents account for the vast majority of vulnerabilities received by *the Company* and follow the standard Product Security workflow. Incidents within this classification are normally already public information or originate with a known researcher(s) or security partner(s) and have a well-coordinated embargo (if applicable). Minimal or no specific customer awareness activities or executive briefings are required. Additionally, SLAs for resolution are sufficient enough to prevent rushed or escalated response activities.

While typically, a minor incident would be of low or moderate severity, it is possible that a vulnerability with an important or even a critical severity rating could be classified as a minor incident, given the right circumstances.

The graphic below displays the workflow for a minor incident.



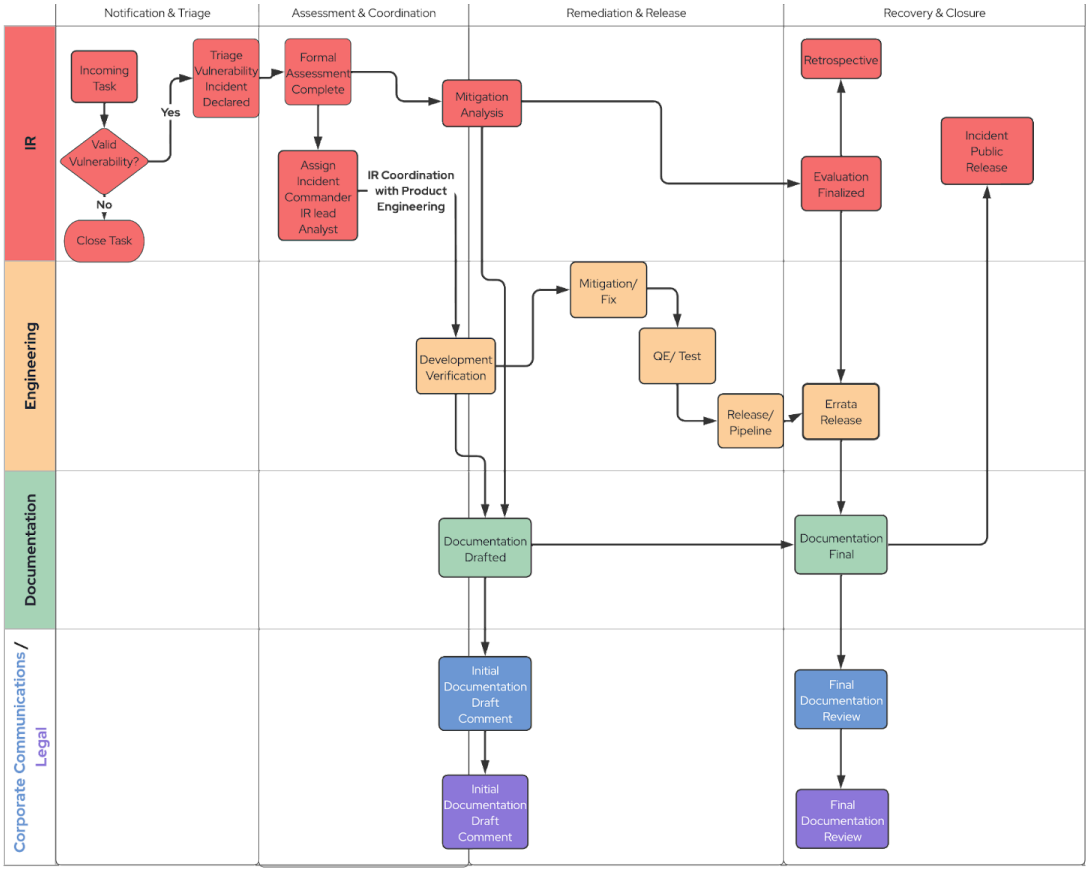
4.2 Major Incidents

Major incidents are defined by their potential visibility to external stakeholders, media coverage, public outcry, the complexity of the vulnerability, higher severity ratings and/or a higher risk to our customers or

the ecosystem. Major incidents will almost always involve critical or important severity vulnerabilities where timelines for resolution are shorter, and multiple offerings may be affected. Additional implications to consider are whether there is existing external coverage and whether previously alerted customers are impacted or potentially impacted. Executive briefings and coordinated internal and external communication are required.

The addition of these requirements and complexity requires additional oversight and orchestration by a Product Security Incident Commander, Incident Program Manager, Product Security Incident Response analyst, and other key players. Occasionally, a major incident will require even more coordination, specifically among executive management. These major incidents with executive- level watch required have severe direct impact on *the Company's* core offerings.

The graphic below displays the workflow for a major incident.



4.2.1 Declaring Major Incident

During the formal assessment, the incident response team will review and determine if the incident meets the criteria for a major incident. When the criteria below are met, incident response's initial triage or formal assessment functions trigger the major incident process within the vulnerability tracking tool. All major incidents or embargoed incidents require a centralized orchestration effort to provide a corporate response addressing the issue for *the Company's* customers.

Determination of a major incident:

- A critical, important or moderate severity vulnerability that meets one or more of the following criteria:
    - Potential headline issue or branded vulnerability.
    - Affects a major *Company* platform or infrastructure.
    - Affects multiple *Company* offerings.
    - Has the potential to cause severe impact, damage or disruption to *Company* customers, employees or infrastructure.
    - Increased customer service requests on the vulnerability.

    - Contains a component that has previously been declared a major incident.
    - Potential public proof of concept or active exploitation.
    - Has cross industry coordination under embargo or via a coordination center, such as CERT-CC, with resulting high-profile security bulletins being released.
    - Is a known exploited issue.

Some major incidents will require **executive level watch**, these incidents will meet the above criteria and the following:

- A critical severity and one or more of the following:
    - Affects a large part of *the Company's* portfolio.
    - Catastrophic impact, damage or disruption to *the Company's* customers, employees or infrastructure or affects *the Company* ecosystem. Severe risk/impact to *the Company's* brand.
    - Requires compensating or mitigating controls within 24 hours.
    - Requires a public response or comment prior to a remediating fix being ready for release.
    - Requires all available resources and the participation of executive management.

4.3 Incident Deliverables

Incident Response management is a core function of Product Security and is key to maintaining *the Company's* overall product security posture. Deliverables of the Incident Response Plan are direct outcomes of the work led by Incident Response with key stakeholders.

4.3.1 Resolution of Vulnerability

For each identified vulnerability, regardless of incident level declared, Incident Response creates tracking tickets for each affected offering. Product Engineering teams prioritize these trackers, determining the best solutions for remediation and complete the work within the allotted SLA, closing the trackers, and publishing the vulnerability remediation.

The Company's security policy dictates that all vulnerabilities with a critical, important, and moderate severity are resolved in accordance with customer-facing product life-cycle documents. Vulnerabilities with a low severity may be resolved in the next major or minor release. *The Company* supports open source ideals with public transparency in providing information.

4.3.2 Communications Internally and with Partners

Internal communication is necessary to inform appropriate internal stakeholders of major incidents. Most minor incidents are less of a concern to stakeholders and do not need formal internal communication.

Deliverable	**From**	**To**	**When**	**Description**
Communication for premium customers	Incident PgM w/ support from Product Engineers	Technical Account Managers, Customer Success Managers	As fix is completed	Talking points and email communications for premium customers
Communication to Information Security	Product Security	Information Security	As a major incident is declared	Ensure affected internal systems are identified and patched
Customer Support FAQs	Incident PgM w/ support	Customer facing associates	As fix is completed	FAQ and/or talking points provided to Support and

	from Product Engineers			Delivery to assist the customer support team answering customer inquiries which require Product Security help to answer.
Insights Team Artifacts	Insights	Multiple *Company* Teams	As a major incident is declared, as appropriate for minor incidents	Insights rule Vulnerability detection script Ansible playbook Customer case auto-comment *The Company's* vulnerability analysis
Major Incident notification (All *Company* Email)	Incident PgM	announce-list distribution	As fix is completed	Provides internal awareness to *Company* associates, ensuring customer-facing associates are informed of the incident in timely manner
Pre-Announcement email for embargoed incidents	Incident PgM	The *Company's* Internal Key Stakeholders	24 hours before all embargoed incident releases	Provides advance notice to certain crucial *Company* stakeholders of an upcoming security vulnerability and what preparation The *Company* has been doing to respond to it.
Translation of the Security Bulletin	Translation Team	*Company* Customers	24 hours before Security Bulletin release	Provides translations of the *Company's* Security Bulletin.

Customer-facing associates need to be prepared to handle customer inquiries about how *the Company* responds to vulnerabilities within offerings. Incident Response along with Product Engineering and other key technical experts, will collaborate to ensure that *the Company's* customer-facing associates are provided the technical information, appropriate formal responses, and supporting documentation to respond to these inquiries. This includes customer support FAQs, notifications/emails and talking points to assist when communicating with customers.

Additionally, incident response will ensure that Information Security and other internal stakeholders are notified of major incidents as appropriate. This ensures that affected internal systems are also identified and patched.

4.3.3 Incident Response External Communication Release

Security Advisories (SA) are developed to accompany the release of an errata for all vulnerabilities, regardless of severity, and are the primary notification system for customers. In addition to SAs, Security Bulletins (SB) are published for all major incidents. CVE pages provide authoritative vendor reference material for each CVE affecting t*he Company's* products. *The Company's* non-product offerings are maintained by *the Company* and therefore do not have published public vulnerability information.

Deliverables	**Description**	**Content Development**	**Review /Release**
Blogs on Security	Technical blogs published on *the Company's* security channel	Product Security associates	Tech Writer Corporate Communica

			tions
Customer email	As necessary, this email notifies the customer segments using the offerings impacted by the security vulnerability. The email is a summary of the issue that directs customers to the comprehensive *the Company's* Security Bulletin so they can take the next appropriate steps.	Incident Commander	Secure Engineering Director
CVEs	All *Company* vulnerabilities. Includes: ● Doc-text Description ● Mitigation Statement ● Impacted Products (Statement) ● External References ● Acknowledgements ● CVSS Comments	Incident Response Tech Writer	Incident Response Tech Writer
Knowledge Base	Secure Engineering coordinates with Support Delivery to provide additional technical articles for vulnerabilities if deemed necessary by the specific vulnerability	Support Delivery Incident Response	Incident Response Tech Writer
OVAL/CVRF/ Security API	Automated feed from *Company* CVE page which provides customers and partners with information regarding the affected state of our *Company* offerings	N/A	N/A
Press Release	Product Security provides a press response for security vulnerabilities that are branded or that are expected to receive media/press attention to proactively address the press/media concern/inquiries on the vulnerability. Note: Only used for high-profile major incidents requiring executive watch.	Incident Response Corp Comms	Product Security Mgmt
Security Advisory	All published Security Advisories (Errata), containing information about impacted products, updated packages and links to other resources	Incident Response Product Engineering	Tech Writer
Security Bulletin	The Security Bulletin provides *Company* customers, Industry Partners and the Media with a comprehensive response to security vulnerabilities and/or Major Incidents. The Security Bulletin provides in-depth, detailed information about the vulnerability, including, the background on the vulnerability, how the vulnerability impacts *Company* offerings, the risk the vulnerability poses to *Company* products and offerings, potential mitigation options and links to the insights deliverables. This document is created for: 1. All major incidents 2. Product major releases a. Summary of fixes and related CVEs	Incident Response (Major Incidents) Tech Writer (Product releases) Insights (Major Incidents)	Incident Commande r (Major Incidents) Tech Writer (Both)

SEO Tactics and Key matches for Security Bulletin	In order to help customers find the appropriate articles for their needs, Product Security helps identify a list of keywords within the vulnerability article to help internal and external search engines index the article appropriately. **Keymatches:** ● CVE number(s) ● Technical Vulnerability name ● Affected offerings list ● Alias and different variations for terms Note: Only used for high-profile major incidents requiring executive watch.	Tech Writer	Tech Writer
Translation of the Security Bulletin	*Company* customers are geographically and culturally diverse, therefore the *Company's* translation team will translate the final Security Bulletin. Translated content is just another service *the Company* offers to increase the value we provide our customers for security vulnerabilities. The translation is posted along with the Security Bulletin in the Customer Portal.	N/A	Translation Team
Twitter Security	Additional forum to notify customers of *the Company's* response to a security vulnerability. Directs customers to technical blogs, featured security content, and The *Company's* Security Bulletins.	Product Security associates	Twitter Admin
Vulnerability Center Banner	The purpose of the vulnerability center banner is to highlight *the Company's* response to a vulnerability on the Product Security Center site in the customer portal. This banner is viewable to *Company* customers and associates logged into the customer portal. Note: Only used for high-profile major incidents requiring executive watch.	Tech Writer	Tech Writer
Zero Minute notification	Special email notification sent out via automated feed from *Company* CVE pages to selected customers whenever a critical severity or major incident vulnerabilities are un-embargoed	N/A	N/A

5 Incident Handling

5.1 Incident Response Phases

The Company's Product Security Incident Response follows four phases in the incident response process to generate a resolution for each reported vulnerability.

This section focuses on the high-level process of each phase and follows the vulnerability through the relevant steps in the four incident response process phases:

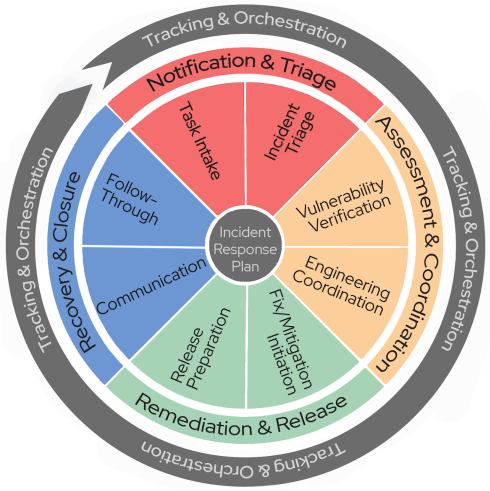


Figure 4

5.1.1 Notification & Triage

Incident Response Triage obtains, filters, and investigates information about security concerns that may affect *the Company's* offerings, leading to the creation of tasks and incidents feeding into the formal assessment process. The incident response process begins when the potential vulnerability is validated as affecting a *Company* offering(s). A flaw is created from the task ticket, and an incident is declared.

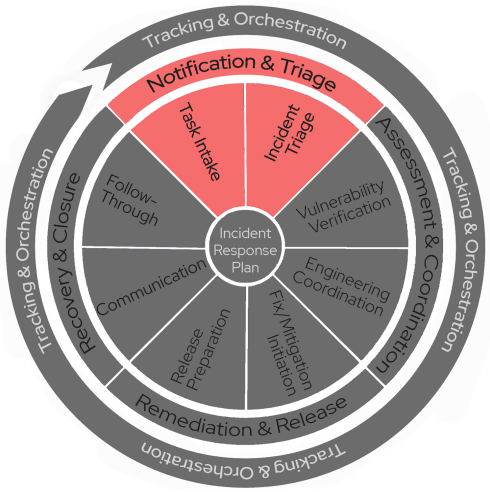


Figure 5

5.1.1.1 Task Intake

As *the Company* and the communities work to review and improve open source software, potential issues are discovered. Intake and reporting are the single point of entry for external entities to present potential vulnerabilities to *the Company* and for *the Company* to receive the potential vulnerability for triage.

Task intake relies on a twofold approach. Automation monitors public internet sources relevant to the security of upstream components, and aggregates these “feeds” for analyst review. Additionally, a public-facing manual ticketing system (the contents of which are restricted to Product Security) provides for the private- and optionally encrypted- transfer of sensitive information.

In this first phase of the Incident Response process, Incident Response will obtain information on potential vulnerabilities from the finder or other external sources to triage, assess/verify, and determine the initial impact on *the Company's* offerings.

5.1.1.2 Initial Triage

After determination that a vulnerability, weakness or other valid security concern is present, initial triage is performed to determine all affected *Company* offerings and dependencies. This information is documented. Incident Response triage works through the following:

1. **Validate the Vulnerability and Determining Affected Offerings**
   During initial triage, a standardized process determines if the potential vulnerability has any effect on *Company* offerings and if so, the vulnerability is validated. Once validated, the vulnerability is tracked within *the Company's* flaw tracking system, noting all affected offerings. This allows consistency in triage, assessment and orchestration for all vulnerabilities.

   As part of this effort, analysts will work to identify the affected products, layered products, containers, and which *Company* Services are potentially affected.

   If it is determined that the vulnerability does not directly impact *Company* offerings, the information is documented and the issue will be closed. Analysts follow the Reject a CVE process if the determination is made during triage to reject the CVE.

2. **Assess Initial CVSS score, CWE, and Severity Level**
   Analysts from Incident response calculate the CVSS score, identify any appropriate CWEs, and assign an initial *Company* severity level of either Low, Moderate, Important, or Critical. This severity rating can be changed later based on the impact on individual offerings.

   Incident Response makes an initial classification of the incident as major or minor based on the information acquired during initial triage, the CVSS score, and severity level. All major incidents meet certain criteria laid out in the Major Incident documentation.

3. **Assess Embargo**
   If the vulnerability was reported to *the Company* under an embargo, Incident Response ensures the vulnerability is flagged as an embargo within internal documentation and tracking tools to prevent leakage of embargoed data.

4. **If required, allocate a CVE**

5. **Provide initial documentation of the security issue and further reference information**
   Technical notes start as soon as the initial triage process begins. This information is noted in the flaw and is used by Incident Response and Secure Engineering for further assessment.

5.1.2 Assessment & Coordination

During the Assessment & Coordination phase, Incident Response completes a formal assessment and provides results to other stakeholders to determine the best possible solution to remediate the vulnerability. Secure Engineering continues its investigation after initial analysis to gain a full understanding of the vulnerability, vulnerable code, possible mitigations and identifies any potential actions, which assist in providing a solution for our customers. This information is noted within trackers. The information gathered during initial triage is validated, an in-depth technical assessment of the vulnerability is completed, and initial mitigation solutions are determined for the offering(s).

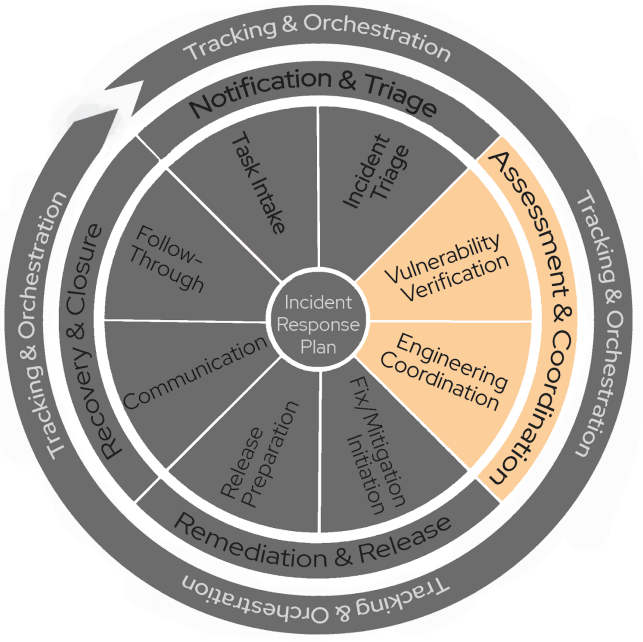


Figure 6

5.1.2.1 Vulnerability Verification

For all incidents, regardless of the classification, Incident Response performs a deeper investigation of the reported vulnerability, confirming all relevant information on the flaw, performing technical analysis, and updating the vulnerability information reported in the flaw. The analyst:

- Ensures task and flaw information is current and correct.
- Creates trackers for all affected offerings.
- Confirms or identifies reproducers and mitigations, where needed.
- Writes flaw descriptions and statements.

The following items must be provided or verified in collaboration with other analysts and engineering (for procedural details, refer to the Formal Assessment - Flaw analysis workflow) .

Item	Notes
Validation of Major Incident	If a major incident has been declared, key stakeholders within Incident Response collaborate to decide whether the vulnerability warrants the orchestration of a major incident.

Affected offerings	During assessment, the set of potentially impacted offerings (products, layered products/containers, services, and internal pipelines) is verified and updated where necessary. An engineering tracker is then raised for each offering assessed as actually impacted so that the fix can be tracked and started.
CVSS score	The following CVSS guides are used to score each flaw: ● first.org CVSS user guide - a short overview ● first.org CVSS spec - detail for each Base Metric ● first.org CVSS examples - detailed reasoning for a broad range of flaws ● first.org CVSS calculator
CWE	The flaw's CWE (Common Weakness Enumeration) is reviewed and set with guidance from Product Security.
Documentation	During analysis, Incident Response begins drafting the flaw's initial documentation, which provides an overview of the incident and *the Company's* planned response. Teams continue to develop documentation as the incident is orchestrated through the Incident Response Process. ● The documentation explains the vulnerability in the specific context of *Company* offerings and describes the impact in a human readable manner. ● A vulnerability impact statement is provided to the public, including an interim mitigation or mitigations that can be applied immediately. ● If the CVE is not embargoed, a CVE page is added to *the Company's* public site.
Mitigation	Incident Response works with Product Engineering to determine potential mitigations for the vulnerability. **Mitigation statements are provided for critical, important, and moderate vulnerabilities.** Potential mitigations are as follows: ● Full/complete mitigation - Removes the threat of the vulnerability to a targeted host, potentially at some impact to the application - such as loss of functionality, performance, or availability of the software. ● Partial mitigation - Reduces the impact of the severity of the vulnerability, albeit with some potential impact. ● No known mitigation - A mitigation to reduce the threat is unknown.
Severity	The flaw's security is reviewed and set following the internal security ratings guide.

5.1.2.2 Engineering Coordination

Product Engineering Engagement

As Incident Response finalizes the assessment, Product Engineering, Quality Engineering, and Release are engaged to perform the work necessary to remediate.

- Through the flaw, Incident Response provides any necessary analysis and information, including upstream patches or release notes, mitigations, analysis notes, and any flaw reproducers (with appropriate security).
- Through the engineering trackers, Incident Response provides an initial timeline and clear expectations of milestones for remediation development, testing, and release.
- The engineering trackers are also a safe conduit for information exchange between Product Security and Engineering, wherein the Engineering teams can propose to reject, rescore, or rebuff the security issue.

Identifying Remediations

Product Engineering works to identify any additional offerings that may be affected and starts to develop the code to mitigate and remediate the vulnerability. Product Engineering expects to manage its resources and priorities to meet the customer needs for timely resolution of all incidents.

Major incident expectations are provided as soon as a major incident is declared to ensure existing priorities and commitments for the impacted product teams are managed appropriately. Product Engineering needs to negotiate changes to other release plans or negotiate with Incident Response on an alternative timeframe that is acceptable to all parties - such as releasing the updates after it is public if changes to the milestones and timelines are necessary.

Product Engineering is expected to be fully engaged with Incident Response and Secure Engineering to gain as much insight into the issue as possible. If required, Product Engineering will also work with industry peers, security researchers, or upstream to confirm resolution.

5.1.3 Remediation & Release

At the beginning of the remediation phase, Incident Response has a full listing of impacted offerings and trackers have been created during the triage phase and validated during the assessment phases. During remediation, Secure Engineering will work with impacted stakeholders to implement appropriate compensating controls and/or develop and complete a remediation fix for the flaw. Once the fix is complete, tested, and prepared for release, documentation noting the security vulnerability, remediation and follow-up will be finalized.

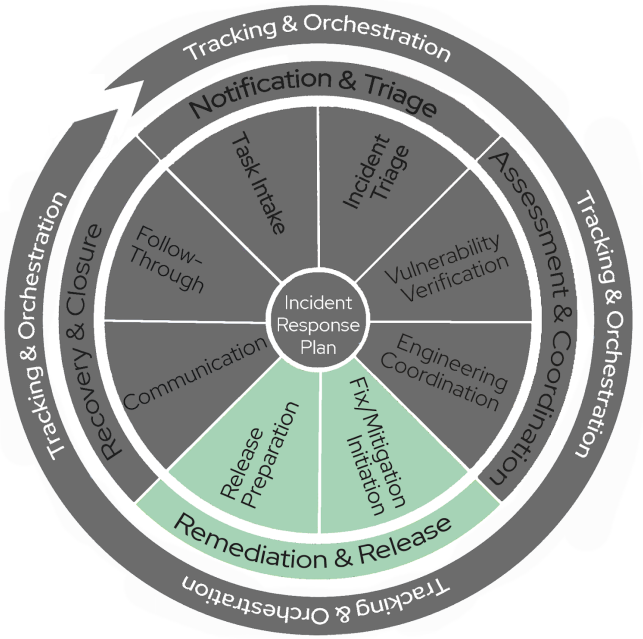


Figure 7

5.1.3.1 Fix/Mitigation Initiation

Product Engineering assesses the vulnerability against their own release criteria and applies fixes within offerings code repositories. Product Engineering creates patches/fixes and performs basic validation that the fix will resolve the vulnerability. If a fix is not necessary and policy allows, Product Engineering closes the trackers, noting in detail why remediation did not occur.

QE is expected to start preparing their test plans, reviewing or creating reproducers and regression/functional coverage, and be ready for testing content when provided by Product Engineering.

Product Engineering passes the content which will fix the known vulnerability to QE, and the trackers and their associated fixes are attached to an errata to track for release.

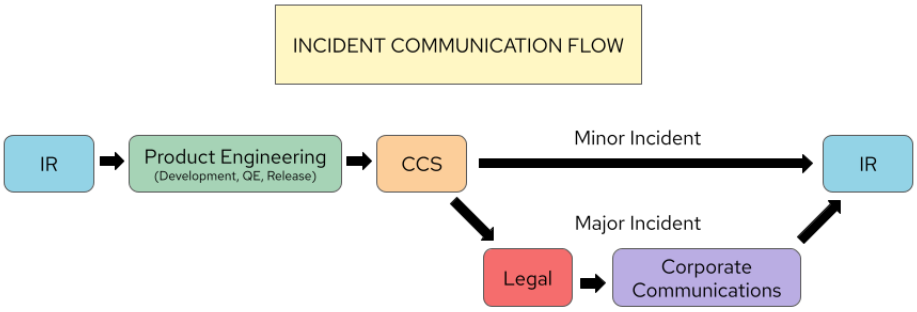
5.1.3.2 Release Preparation

Testing

QE is expected to prepare and execute a full suite of tests that ensure regression and functional testing is performed, along with validating that the CVEs are fixed - using any reproducers or information available to confirm the patches are applied and functional.

Final Reviews of Documentation

Incident Response and additional approvers complete a final review of the documentation for the specific release.



Release Errata
When a fix is ready for release, the fix is verified and QE confirms completion within the errata tool. Documentation specific to that fix is attached. Release Engineering releases the fix and software updates, along with the corresponding documentation using errata tool.

A Product Security Manager approval will be requested in order to approve releases on black-out dates.

5.1.4 Recovery & Closure

Recovery is the final phase of the incident response process. Actions in this phase ensure all incidents and sub-tasks within the incidents have been thoroughly documented and closed. In addition, all formal communication will be finalized and released. Incident follow-through will occur ensuring proper retrospective and closure of the incident.

For a major incident, several activities will occur in the final 24 hours before disclosure of the incident. The majority of these activities assume that the incident is under embargo towards a 'Coordinated Disclosure.' Where no embargo is happening, the timelines are usually much shorter, with the aim to release as soon as possible based on an agreed timeline.

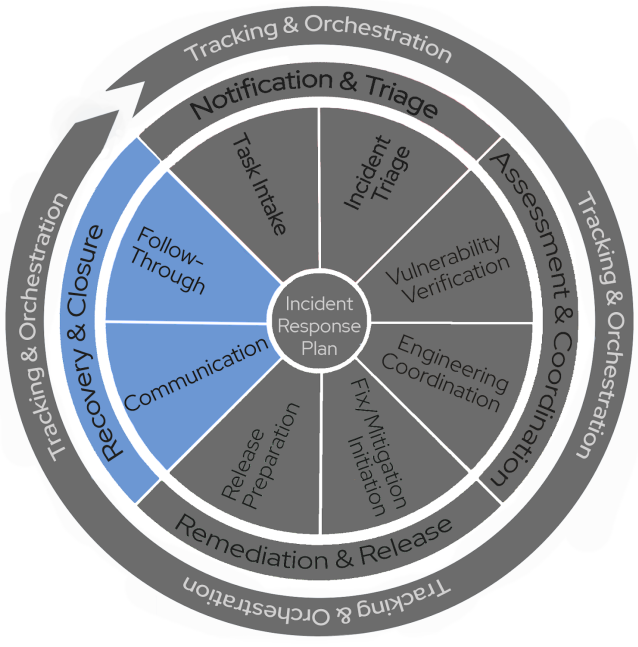


Figure 9

5.1.4.1 Communication

Update Communication Channels

Incident Response ensures all internal and external communication has been updated, finalized and released via the appropriate channels.

5.1.4.2 Follow-Through

Tracking

Ensure all incident information is documented in the appropriate ticketing system. All actions need to be noted in the tickets, including impact, remediation, testing, and detailed documentation, including the reasoning for any vulnerability not fixed.

Retrospective

The retrospective is a feedback loop which seeks to improve our Incident Response Plan for future events and to provide feedback addressing challenges to other stakeholders in *the Company.*

5.2 Incident SLA

Timing is critical when responding to incidents. Vulnerabilities must be addressed in a timely manner. SLA times start when initial triage analysts on Incident Response receive notification of the vulnerability. For the current SLA guidelines, refer to *the Company's* Security Errata Standard.

6 Stakeholder Expectations and Communication Methods

Incident Response requires good coordination and communication both internally and externally to *the Company* to ensure that all stakeholders are well informed and teams collaborate well. Having well defined expectations and communication methods is key to providing information to each stakeholder in a consistent manner.

Communications provides the external messaging to non-customer audiences, including journalists, technology sector analysts and other influencers. Messages are derived from the internal and customer-facing content created by Product Security.

Communications content includes *Company* blog posts, social media posts from primary *Company* platforms and rapid response emails to journalists/analysts.

6.1 Incident Response Orchestration of Major and/or Embargoed Incidents and Key Roles

6.1.1 Orchestration

The IR team is responsible for the analysis of new, potential vulnerabilities affecting *the Company's* offerings portfolio. The following roles are key within IR, focusing on the initial triage, formal assessment, and orchestration of Major Incidents.

Incident Commander:

The Incident Commander (IC) is the technical focal point and the technical decision maker during a **major incident and/or embargoed incident.** This includes delegating tasks and seeking and listening to input from subject matter experts to bring the incident to resolution. The IC delegates all activity-level actions or remediations, such as writing code or investigating logs. Information pertaining to all security incidents is tracked in the Incident Response Dashboard. The IC should also actively consider next steps and backup plans at every opportunity to keep things moving towards resolution.

Incident Response Program Manager:

The Incident Program Manager (PgM) is responsible for the managing and **Orchestration** of incidents from beginning to end. The Incident PgM will ensure that all active incidents, including embargoes are tracked from initial notification through closure. While the Incident PgM has a purview of all incidents, the focus is on the coordination of major and/or embargoed incidents.

The Incident PgM works to ensure appropriate communications channels are established, coordination documents are maintained, and executive briefings are created as required. They are also responsible for coordinating all release communications with appropriate stakeholders, such as *the Company's* content services, corporate communications, and legal teams.

Incident Response Analyst:

The IR analyst is responsible for the **Initial Triage** of all incoming incidents during the Notification & Triage phase of the Incident Response process. The analyst reviews assembled data from external sources, and creates the vulnerability task. If the flaw is a clear threat to *Company* offerings, a matching flaw bug is also created and the analyst does an initial assessment of severity, CVSS, CWE, as well as using manifest data to determine affected offerings. Based on the initial triage of the vulnerability, impact and risk to *the Company*,

the analyst proposes to declare a major incident if the criteria are met.

IR analysts are also responsible for the **Formal Assessment** of the vulnerability during the Assessment & Coordination phase of the Incident Response process, including:

1. Validating the analysis of the incoming analyst, including: ensuring the CVSS score is appropriate and does not need to be rescored; the CWE is correct; and the severity is accurate; a major incident is declared as appropriate.
2. Ensuring that the set of affected offerings is complete.
    a. If necessary, additional product security analysts are notified to validate all potentially impacted offerings, including layered products and containers.
3. Coordinating with Product Engineering on the technical aspects of the vulnerability, prioritizing unresolved vulnerabilities, and engaging proactively on the overall security architecture of the offering (for example, by performing offering reviews and audits).
4. Writing flaw descriptions and statements for the CVE page, SBs and SAs as appropriate.

If the vulnerability is under embargo or warrants the orchestration efforts of a major incident, the lead analyst functions as the incident lead and collaborates with the Incident PgM and the IC. This effort also involves coordination with the finder and any other external parties as necessary.

6.1.2 Incident Response Orchestration Playbook:

The team organized to respond to major and/or embargoed incidents will complete tasks as outlined in the IR Orchestration Playbook. It is the responsibility of the Incident PgM to ensure the playbook is used for all incidents and is maintained with all incident documentation on the Incident Response shared drive.

6.2 Internal Stakeholders

It is important to note that some responses necessitate a joint approach across *the Company*, requiring input from Product Security, Information Security and additional stakeholders. When applicable, Product Security will work with the appropriate teams to ensure any vulnerability is addressed adequately.

6.2.1 Information Security

The Company's Information Security is responsible for the security and safety of *the Company's* corporate infrastructure. All incident handling within *the Company's* corporate network will be coordinated and remediated by Information Security through the Information Security Incident Response Team (ISIRT). Product Security Incident Response and ISIRT often share information on vulnerabilities and work together to provide joint responses.

Security incidents not only impact our customers using our Offerings but also impact our own usage of our offerings internally. Information Security provides organization and coordination services for Information Security incidents, both within *the Company's* corporate environment and customer environments, i.e., Managed Services. See Information Security's Incident Response Plan.

Information Security will feed vulnerability information found in their scans to Incident Response using the secalert@company.com distribution. This alert will notify the Incident Response management and will be routed through Incident Response triage if appropriate.

Conversely, Information Security will be notified of remediation options for *the Company's* offerings and coordinate remediation efforts with internal stakeholders throughout the business and internal system domains via the infosec-admin@company.com conduit, for issues potentially affecting from www.company.com, to corporate infrastructure, to associate endpoint systems.

Information Security will review communication about vulnerabilities within *the Company's* offerings to ensure the message is clear among *the Company's* associates and *the Company's* customers. In addition, Information Security will review any communications regarding the status of internal *Company* services or systems to *the Company's* customers.

6.2.2 Product Security Supply Chain

Product Security Supply Chain (PSSC) has a holistic understanding of *the Company's* software supply chain infrastructure. They will work with engineering teams who maintain the services, tools, and infrastructure operating in *the Company* with the ability to manipulate code during the build process of the offering.

Product Security Supply Chain is tasked to provide guidance and insight on how *the Company's* Productization Pipeline will continuously place efforts to improve and protect *the Company's* pipeline's security posture. PSSC will guide detection efforts once an incident begins by researching potential impacts to the PPC (i.e. what tools do we use that might carry the vulnerability). To ensure this research occurs, the Incident Commander should reach out to the PSSC leader advising them that there is an incident that potentially involves the Software Supply Chain.

6.2.3 Engineering Team Responsibilities

6.2.3.1 Product Engineering

Product Engineering develops and delivers software content and management tools for *Company* offerings. In addition, Product Engineering educates, supports, and collaborates with upstream projects and other *Company* teams.

As part of the CVE process, product engineering has the following responsibilities:

- Notify secalert@company.com when development issues arise which might impact product security.
- Respond to technical product queries by Product Security
- Receive and own development trackers raised by IR for the update of the flaw, and:
    - Analyze the flaw's impact with particular respect to the tracker's product.
    - Evaluate and prioritize the tracker, using *the Company's* Security Errata Standard as guidance, ensuring that trackers are handled within time frames defined by *the Company.*
- Update product to fix the flaw. During development:
    - Use secure development practices to ensure product updates are securely developed and do not introduce regressions.
    - Use EXD policies and procedures to ensure the supply chain is well secured.
- Deliver product updates to the Quality Engineering team in a timely manner.
- Where needed, create errata for update release:
    - SA created for security releases
    - EB and SB are created for enhancements or bug fixes; SB/EB can also include security fixes if necessary.

Outcomes

- Updated build delivered to Quality Engineering for testing.
- Where needed, technical advice given to Quality Engineering for testing the update and validating the fix.

Note: Product Engineering is not responsible for any documents involved in the CVE process.

6.2.3.2 Quality Engineering

Quality Engineering writes, plans, and executes tests for *Company* offerings, so that these function well

and meet customer requirements. Quality Engineering might also design and maintain the testing infrastructure.

As part of the CVE process, Quality Engineering has the following responsibilities:

- Access reproducer advice from Product Security, where available.
- Receive technical advice and offering updates from Product Engineering.
- Create test requirements, plans, and cases for offering updates, following *Company*-defined best practices.
- Execute update tests in a timely manner, validate the fix, and ensure regressions are not introduced with the update. Deliver test results to both Product Engineering and Release Delivery in a timely manner.

Outcomes

- Testing reports or results delivered to Product Engineering and Release Delivery.
- Any documents used for update testing.

6.2.3.3 Release Engineering

The Release Engineering team releases content for *Company* offerings for the community, developers, testers, and customers. The team operates, maintains, and develops tooling and services for software delivery.

As part of the CVE process, Release Engineering has the following responsibilities:

- Receive updated and verified build from Product Engineering.
- Where needed, create errata for product-update release:
    - SA created for security releases
    - EB and SB are created for enhancements or bug fixes; SB/EB can also include security fixes if necessary.
- Release updates through appropriate channels (for example, erratum, ftp hot fix, or container catalog).
- Ensure container catalog Health Index is maintained with appropriate grades, including recreating containers to include released security fixes.

Outcomes

- Erratas published, shipped and finished with approvals from both Product Security (CVE information) and Customer Content Services (errata documentation). Product updates released.

6.2.4 Customer Content Services (Tech Writer)

The Customer Content Services-for-Product Security (CCS4PS) Team is responsible for the curation, editing, and publishing of information that is meant for the public audience. This includes security bulletins (SB), vulnerability articles (KCS), doc-texts, and documentation for Product Security projects such as Supply Chain Management.

In the event of a leak/embargo break, communications is also responsible (if needed) to spin up reactive statements to “tide us over” until formal content is ready.
From a documentation review, communications should review customer portal posts, external blog posts and critical emails (customers, key partners) simply as part of the general workflow.

6.2.4.1 Security bulletin

CCS4PS works directly with the Incident Commander and Incident PgM for major incidents to create the necessary documentation required to meet the needs of the customer. This usually means the creation of a SB which includes information that is useful to all levels of people.

When notified by the Incident Commander or Incident PgM of a major incident, CCS4PS collects the following information to begin the response:

- CVE number
- Incident ticket number
- Documentation ticket number (if one has been created)
- Date and time (with timezone) when the embargo is scheduled to be lifted
- Main Incident Response analyst working on the issue.

The SB should be created from the template managed by CCS4PS. Vulnerability information from the flaw bug will be documented in the SB. Once this information is collected, CCS4PS shares the SB with the Incident Commander, Incident Response Analyst, Incident PgM, and the rest of the CCS4PS team, and creates a schedule for sign-off reviews.

During major incidents, CCS4PS coordinates with the Incident Response analyst(s) responsible for developing the technical language describing the vulnerability, which will become the language in the security documentation.

Recommended changes to the document are also consumed as they come in from corporate communications, legal, and others. All modifications to the SB should be completed prior to one business day before the release of a fix for the vulnerability or the embargo is scheduled to be lifted.

When the security bulletin is complete, CCS4PS reviews the document for grammar, spelling, and readability and then moves the document into the Portal for final markup. Once finalized, the information from the SB will be copied over to the flaw bug so that all information published to the public matches.

For security reasons, in the case of an embargo, this movement into the Portal should not happen more than 24 hours prior to the lifting of the embargo. The executive summary becomes the doc-text for the vulnerability and the mitigation becomes the mitigation statement in the bug. These texts should be the same, wherever possible, to prevent confusion from differing instructions.

At embargo lift time, upon the instruction from the Incident Commander, a member of CCS4PS may publish the SB. The SB must not be released prior to instruction from the Incident Commander to avoid breaking the embargo

6.2.4.2 Vulnerability Articles

CCS4PS works directly with Product Security associates to review the language and readability of Vulnerability articles (published in the *Company* KCS). Once ready for review by CCS4PS, the author drafts the article and creates a ticket for review by CCS4PS (prodsec-content@company.com) in the Incident Response Tracking Tool.

6.2.4.3 Doc Text

CCS4PS is responsible for the review and approval of Doc Text field in the Incident Response Tracking Tool - which is the content that will be shown in the CVE pages. Mitigations and statements are also reviewed for spelling, grammar, and readability. The SLA for Doc Text is dependent upon the Severity Rating and is as follows:

- Critical impact - 1 business day
- Important impact - 1 business day
- Moderate impact - 5 business days
- Low impact - 5 business days

6.2.5 Legal

Company Legal examines applicable local, state, federal and/or international laws, contractual obligations, and other potential legal exposures, risks and considerations associated with security vulnerabilities reported or discovered within *Company* offerings. Depending upon the particular context and specifics, legal

considerations and responsive actions may include the following:

- Coordinate efforts to manage regulatory requirements and notifications associated with security vulnerabilities reported or discovered within *Company* offerings.
- Review applicable federal, state and local laws and develop an appropriate course of action to comply with such laws, particularly in the event a data exposure occurred.
- Document the types of information that may have been exposed or compromised, if any.
- In the event of a data exposure, ensure all aspects of a data exposure management plan and applicable privacy laws are properly and fully addressed.
- Coordinate activities with *Company* Information Security, including their Global Privacy Program.
- Throughout the investigation process, provide guidance on issues relating to liability, compliance, records management, regulatory requirements, contractual obligations, and privacy and confidentiality of customer and employee personal and business information. Assist in developing appropriate internal and external communications, including those to any impacted customers, regulators, partners, other parties and the public.
- Assess the need to change policies, procedures, and/or practices as a result of the vulnerability.
- Assess and manage required regulatory notifications.
- Provide legal counsel for response and recovery operations.
- Engage and coordinate external legal resources, including outside counsel, consultants and law enforcement, if necessary or appropriate. Consider the need to review existing contracts or modify new contracts as a result of the event.
- Assess impact of prior incidents and disclosures.
- Facilitate employee training and tabletop exercises.
- Evaluate the need to notify any insurance carrier.
- Participate in communications with relevant internal and external groups to address confidentiality and embargo related considerations. Craft strategies and submissions on public policy issues and positions.
- Ensure that Product Security is compliant with current branding and messaging standards as well as the regulatory/legal environment (e.g., privacy, federal space).
- Determine what information can be collected and how long it can be kept.

6.2.6 Corporate Communications

- Communications provides the external messaging to non-customer audiences, including journalists, technology sector analysts and other influencers.
    - Messages are derived from the internal and customer-facing content created by PSIRT.
- The Communications team is generally alerted early on in the process, though communications' deliverables are not created until technical documentation and articles are finalized for internal usage. This group also helps establish whether we should be reactive (only responding to inbound queries) or proactive (actively reaching out to specific targets with our point of view) to press and analysts.
    - Communications content includes *Company* blog posts, social media posts from primary *Company* platforms and rapid response emails to journalists/analysts.
- In the event of a leak/embargo break, communications is also responsible (if needed) to spin up reactive statements to "tide us over" until formal content is ready.
- From a documentation review, communications should review customer portal posts, external blog posts and critical emails (customers, key partners) simply as part of the general workflow.

6.2.7 Product Management and Business Unit

The product management and business unit leaders are directly responsible, ensuring that flaws are prioritized, fixed, and released in a timely manner. The key to this work is making quick decisions on whether flaws are fixed and in which release the fix is provided.

6.2.8 Product Security Development and Operations

The Product Security Development and Operations or “DevOps” team is responsible for maintaining the data and tooling used by the Product Security team. Data is curated through workflow tooling, automation, and backend scripts which ensure proper tracking and generation of customer consumable data. This data is also used to generate metrics used by Product Security and product teams to ensure flaws are tracked and resolved appropriately.

6.2.9 Site Reliability Engineering (SRE - customer 0)

The Company has diverse internal SREs, from CEE, IT, Engineering and potentially other teams with their own infrastructures. These organizations and systems are governed by IT security policies. These teams are responsible for maintaining our hosted products. Historically the Product Security Services team worked closely with these teams.

6.2.10 Executive Management

Directors and VPs of the business units, customer support teams, and the sales organization require briefings early and often to help prepare and lead their teams during elevated incidents. They are responsible for escalating resources and ensuring that customer impact is as minimal as possible. For some major incidents, especially those with significant media coverage, our leadership will need to be aware of what is happening.

6.2.11 Customer Support

The Company’s Customer Support team is composed of both technical and non-technical members who are the frontline response for customer facing issues. The team is responsible for the initial triage, answering, and escalating customer issues. Customer Support acts as a bridge and an advocate for our customers during a major incident. They help to understand the customer's concerns, provide technical support assistance, and access to any needed resources.

In the event of an embargoed incident, support delivery will receive notification from the Incident Response PgM, when appropriate. Typically, a support manager and a support engineer are employed to help assess the embargoed incident. It is the responsibility of these individuals to assess and adequately prepare for the response to the incident. Support and Incident Response will work together to gauge the effect of the incident and the immediate deliverables necessary.
In some instances, information about the vulnerability may leak on the internet, and in these cases, it is imperative that our engineers not make comments regarding the incident and a member of management contact Incident Response immediately for next steps. Communication will be developed in case customers begin to inquire about security incidents. Product Security will review and approve all communication which is delivered to the customer.

6.2.12 Field Teams

Solutions Architects, Consultants, Sales Representatives, Technical Account Managers (TAMs) and Customer Success Executives (CSE) are in close touch with customers and prospect customers, and are an important information conduit. Given the high touch nature of contact with our customers, the Field Teams are, as valued evangelizers to direct consumers of ProdSec information, thus ensuring the proper understanding by the Customers of the impact of a vulnerability present in our products and, being able to diagnose the detailed affectedness of a vulnerability in the customer’s environments. The Field Teams are also engaged in the event of Major Incidents, in order to have timely information and show value for our customers.

6.2.13 Organization Wide (Announce list)

The Company Announce list is used to communicate to all of *the Company* the awareness of a major incident. This information is a kick off for all associates to understand the current impact to our products and where to go for further information and clarification.

6.3 External Stakeholders

It is important to communicate effectively with organizations outside of *the Company*. When applicable, Product Security will work with the appropriate teams to ensure any vulnerability is addressed adequately.

6.3.1 *Company* Subscribers

A subscriber is most generally defined as a customer with an active support subscription. Subscribers rely primarily on and consume Security Advisory (SAs) to keep their systems up to date and secure. Subscribers also utilize the CVE pages for vulnerability descriptions, mitigation detail, and FAQs to help with their own internal security risk management process. Security bulletins (SBs) associated with the Major Incident are tailored to provide easy to understand information for our Subscribers.

6.3.2 *Company* Partners

Partners are defined as independent software vendors (ISV) or independent hardware vendors (IHV) who either build their products on our product portfolio or in the case of IHVs, rely on the success of our product portfolio for their hardware enablement and sales. *The Company* works closely with IHV partners to resolve vulnerabilities based on hardware functionality, which require coordination within our software.

6.3.3 Social Media / Media

As a rule, no one is to talk to the media about our active incidents. After issues are resolved we can refer to incidents in blog posts that have been reviewed appropriately.

The Product Security Management team will post on Twitter a link to Major Incident Security Bulletins and where to find more information.

6.3.4 Finders/Upstream Community/Embargo Owners

The term finder refers to upstream parties and individuals who report a vulnerability either publicly or directly with *the Company*. All finder data is aggregated and triaged by Incident Response. Finders may also wish to keep vulnerability information embargoed with *the Company* and other vendors until a fix is available. In these circumstances, *the Company* coordinates the embargo and disclosure dates with the finder. Finders are recognized on our public CVE pages for valid flaws. The lead analyst is responsible for communicating with these stakeholders for assigned vulnerabilities.

6.3.5 *The Company* Subscriber CSIRTs

A subscriber Computer Security Incident Response Team (CSIRT) refers specifically to a network security incident response organization managed directly by and benefiting a customer. CSIRTs provide large customers with a managed incident approach to security and rely on data that *the Company* provides via our security documentation, including SAs, SBs, CVE, NVD, and OVAL streams to keep their customers as secure as possible.

6.3.6 Industry Incident Response Teams

The Company collaborates with other industry Incident Response teams through organizations such as FIRST or CERT-CC when there are mutually beneficial security objectives.

6.3.7 Third Party Vendors

Third-party vendors include any software vendor which utilizes our security data. Vulnerability scanning vendors, for example, rely on our OVAL data to properly identify flaws with their scanning engines.

Appendix A - Supporting materials and tools

A.1 Policies, Standards and Guidelines

The Company's Product Security publishes and maintains product security policies and standards that are applicable to our entire offerings portfolio.

A.1.1 ISO/IEC 29147 (Vulnerability Disclosure)

This document provides requirements and recommendations to vendors on the disclosure of vulnerabilities in offerings. Vulnerability disclosure enables users to perform technical vulnerability management as specified in ISO/IEC 27002:2013. Vulnerability disclosure helps users protect their systems and data, prioritize defensive investments, and better assess risk. The goal of vulnerability disclosure is to reduce the risk associated with exploiting vulnerabilities. Coordinated vulnerability disclosure is especially important when multiple vendors are affected. This document provides:

- Guidelines on receiving reports about potential vulnerabilities
- Guidelines on disclosing vulnerability remediation information
- Terms and definitions that are specific to vulnerability disclosure
- An overview of vulnerability disclosure concepts
- Techniques and policy considerations for vulnerability disclosure
- Examples of techniques, policies (Annex A), and communications (Annex B)

This document applies to vendors who choose to practice vulnerability disclosure to reduce risk to users of vendors' offerings.

A.1.2 ISO/IEC 30111 (Vulnerability Handling)

This document provides requirements and recommendations on how to process and remediate reported potential vulnerabilities in an offering. This document applies to vendors involved in handling vulnerabilities.

A.1.3 FIRST Incident Response Services Framework

The Services Frameworks are high-level documents detailing possible services that computer incident response teams (CSIRTs) and Incident Response Teams may provide.

Recognized experts from the FIRST [Incident Response] community develop these frameworks. FIRST strives to include feedback from all sectors, including CSIRTs with a national responsibility, private sector CSIRTs, and Incident Response Teams as well as other stakeholders. These documents intend to provide a foundation for the development of new training material. However, today they are used in a much wider scope, for example, when defining an initial service catalog for new teams.

In the creation of the CSIRT Services Framework, it became clear that Incident Response Teams do provide different services and typically operate in different environments. These differences led to creating a separate document covering Incident Response Teams. The documents work in alignment, highlighting the many shared similarities. The development of the frameworks is driven by the Education Advisory Board.

The frameworks exist to assist organizations in building, maintaining, and growing capabilities of their CSIRTs or Incident Response Teams. The Frameworks are guides and identify various models, capabilities, services, and outcomes. In this way, teams are free to implement their own model and to build capabilities that meet their stakeholder's unique needs. The Frameworks seek to assist security incident response teams (SIRTs) by identifying core responsibilities, providing guidance on building capabilities to meet those responsibilities, and offering insights that teams can add and communicate value to their larger organizations.

A.1.4 NIST SP 800-61 Computer Security Incident Handling Guide

This publication seeks to assist organizations in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently. It includes guidelines on establishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing, and handling incidents. Organizations are encouraged to tailor the recommended guidelines and solutions to meet their specific security and mission requirements.

A.2 Central Tracking Operations

A.2.1 Supporting Product Security Incident Response Tooling (Software)

The tools used by Product Security serve two purposes. Those two purposes are internal coordination and metadata tracking (ex. relationships between flaws, offerings, and releases). For internal coordination, our offering teams use the Incident Response Tracking Tool for bug and feature tracking.

A.3 Databases and Data Feeds

The Company uses the following databases, data feeds, and resources to assess the affected state of offerings and to disclose vulnerability data.

A.3.1 CVE Pages

The Company creates and maintains a CVE list via pages in our customer portal. A page is created for each CVE analyzed by Incident Response. Each page provides detailed information on the description of the CVE, mitigation statements, score, impact/severity, and table of affected products. Affected products are limited to the platform level from the portfolio.

These pages are created once the flaw is public and the flaw bug has been created. The page data and affected products table are updated as tracker bugs are resolved and closed.

A.3.2 OVAL

The Company uses the Open Vulnerability and Assessment Language published by MITRE to provide customers and partners with machine-readable data disclosing the affected state of products and packages in our portfolio. These data feeds are organized by major product platforms with streams or files available for each product version. We provide specific streams showing affected and patched CVEs and also streams that include all unpatched CVEs. These streams are maintained for each supported product. However, the entire OVAL repository contains data for supported and unsupported products.

A.3.3 VINCE

For CERT-CC specific vulnerability coordination VINCE is the central tool for tracking, coordination, and communication for an issue that potentially impacts *Company* offerings. *The Company* can provide manual updates and status for vulnerability information impacting *Company* offerings.

A.3.4 National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD)

NIST is the organization responsible for the NVD. “The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP).” *The Company* uses available NVD data such as identifiers and descriptions during initial triage. *The*

Company then completes an assessment of the vulnerability, providing a CVSS score and other pertinent information, based on how our products are built and used. When there are significant scoring differences, we work directly with NVD to consider adjusting their score.