integrity partners
grupa altkom

https://integritypartners.pl

Integrity Partners's approach to software vulnerability handling

Warsaw, 17/08/2020

Vulnerability Handling Policy - Integrity Partners's approach

Index

1. Disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by Integrity Partners (further – IP). IP provides no warranty, express or implied, for the information contained in this document, and assumes no responsibility for the information contained in this document or for any errors that may appear in this document.

2. Purpose

Integrity Partners is committed to providing customers with products, systems and services that address cyber security. In order to minimize risks and impact of breach timely and proper manner of handling software vulnerabilities is considered as key factor for successful cooperation with customer. However, as the system integrator itself in most cases the role in the Coordinated Vulnerability Disclosure process is limited due to contractual responsibilities and business relationships. This document describes Integtity Partners's approach of handling Vulnerabilities from the perspective of System Integrator.

3. Approach procedure

3.1. Overview

IPs approach is based on recommendations and best practices outlined in the "The CERT® Guide to Coordinated Vulnerability Disclosure" [1] issued by Software Engineering Institute from the perspective of System Integrator in the role of "Deployer" defined as:

"The deployer role refers to the individual or organization responsible for the fielded systems that use or otherwise depend on products with vulnerabilities (…) Deployers typically must take some action in response to a vulnerability in a product they've deployed. Most often this means deploying a patch, but it can also involve the application of security controls, such as reconfiguring defensive systems, adding monitoring or detection rules, or applying mitigations."

IP is dependent of other actors in the CVD process (please find in Appendix no. 1). Therefore this policy will be applied mostly in the following events and phases:

- An external party (e.g. customer, researcher, government organization) approaching IP reporting a potential vulnerability [Reporting]
- A vulnerability disclosed publicly [Public Awareness]
- Mitigation fix provided by Vendor [Deployment]

[1] https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf#page=44&zoom=100,0,309

3.2. Vulnerability Response Process

IP's vulnerability response process involves the following sequence of steps:

- Become aware
- Confirm affected systems
- Prioritize response
- Provide remediation
- Test the solution
- Plan the deployment
- Execute the plan

3.2.1. Become aware

In order to take action, IP must know about the vulnerability and have sufficient information to act on. Most often this information originates from the product vendor, but vulnerability information can arrive from other sources as well.

IP will be on the lookout for and pay attention to:

- Vendor security notices;
- Vendor customer support notices (not all vendors provide separate security notices, nor are all vulnerabilities always explicitly called out in update notes);
- Vulnerability and threat intelligence services;
- Security discussions online including social media;
- Mass media coverage of vulnerabilities.

3.2.2. Confirm affected systems

Based on detailed documentation of the vulnerability which were obtained on aware stage in collaboration with reporting entities, IP should provide reproduction of the vulnerability. During this process should be detected all potentially affected systems including 3d party solutions. According to the corresponsive information regarding the vulnerability, IP can start planning and preparation of remediation plan before the corresponsive fix, either patch would be released.

3.2.3. Prioritize response

Approach testing, scheduling out-of-band fixes and planning is required to be discussed and approved with customers in order to respond in effective manner. Draft of the schedule, priorities and decisions taken in this step would impact the steps Test the solution and Plan the deployment.

3.2.4. Provide remediation

Before the Vendor provide official fix and IP would proceed to the solution test stage important to provide remediation activities to affected systems. That can include configuration changes (e.g. disabling of vulnerable service) or recommendations on deployment and configuration of security solutions (e.g. firewalls). IP's goal to provide mitigations if possible to offer customers alternatives to updating a running product immediately. Depending on the severity of the vulnerability and the time needed to develop a software remediation the alternative mitigations might be communicated before the final software remediation is available.

3.2.5. Test the solution

Testing prior to deployment is important if either of the following conditions is true:

- The system's availability and performance are critical;
- Reverting a patch deployment gone bad is difficult.

Every case is discussed with customers affected and approach towards their testing policy and approach is decided taking into consideration for instance automated deployment and rollback capabilities.

3.2.6. Plan the deployment

Planning for a patch deployment requires two major steps:

- Identify and enumerate system instances affected by the vulnerability.
  Taking into consideration tools and repositories such as CMDBs, vulnerability management tools to define the scale of the patching effort required.

- Update and confirm the deployment schedule.
  Taking into consideration prioritized response the deployment approach is confirmed (i.e. first-in-first-out process, scheduled maintenance windows, push out a patch outside of a scheduled maintenance window)

3.2.7. Execute the Plan

Continuous monitoring of the deployment of the mitigation or fix with the customers.

4. Disclosure support procedure

Due to company business specific, Integrity Partners engineers, Cybersecurity experts, architects and any other technical specialists are not providing any vulnerability researches due to their job responsibilities. Nevertheless, due to the close collaboration with the customer acting like a SME in different technologies and systems, some occasionally discovered vulnerabilities might be disclosed with the Integrity Partners employees and service delivery partners. In such case this unknown vulnerability should be claimed to the specific vendor in shortest time, where assigned to case Integrity Partners SME could help the customer prepare a report described in appendix 2 of this document, strictly keeping all the details in total privacy.

In case of any vulnerability discovered by the Integrity Partners Cybersecurity expert, for example during the load and performance tests in personal lab, or any other security assessment exercise, such vulnerability should be claimed in the corresponsive manner using report example in appendix 2. Integrity Partners is the recognized professional organization with the corresponsive high ethics approach, meaning that information regarding discovered vulnerability should be kept in a total privacy till the vendor would disclose that or provide a corresponsive patch.

5. Further considerations.

Integrity Partners issued this policy to be a part of Coordinate Vulnerability Disclosure process acting currently in a Deployer role. Nevertheless considering further business development, meaning attendance as a Coordinator or even a Vendor representative in different cases. Based on Developer role, Integrity Partners leave a permanent right to notify own customers, regarding the already known (disclosed vulnerabilities) after the official Vendor claim (disclosure) in personal manner, as a gesture of good will, using personal template that described in appendix 3 of this document. That is done due to parity trust relationships with the most customers, where company is recognized like a trusted cybersecurity advisory.

Due to the ongoing changes in our organisation and impetuous developing Cybersecurity world, this policy should be continuously reviewed on yearly bases.

Appendix no. 1 – Proposed model of SEI's adapted CVD proces

Phases of CVD process at the CERT/CC based on ISO/IEC 30111 described in "The CERT® Guide to Coordinated Vulnerability Disclosure" 2 issued by Software Engineering Institute:

1. **Discovery** – A researcher (not necessarily an academic one) discovers a vulnerability by using one of numerous tools and processes;
2. **Reporting** – A researcher submits a vulnerability report to a software or product vendor, or a third-party coordinator if necessary;
3. **Validation and Triage** – The analyst validates the report to ensure accuracy before action can be taken and prioritizes reports relative to others;
4. **Remediation** – A remediation plan (ideally a software patch, but could also be other mechanisms) is developed and tested;
5. **Public Awareness** – The vulnerability and its remediation plan is disclosed to the public;
6. **Deployment** – The remediation is applied to deployed systems.

A mapping of CVD phases to CVD roles is provided in Table below:

	FINDER	REPORTER	VENDOR	COORDINATOR	DEPLOYER
DISCOVERY	Finds vulnerabilities				
REPORTING	Prepares report	Reports vulnerabilities to vendor(s) and/or coordinators	Receives reports	Receives reports Acts as reporter proxy	
VALIDATION AND TRIAGE			Validates reports received Prioritizes report for response	Validates reports received Prioritizes report for response	
REMEDATION		Confirms Fix	Prepares patches Develops advice, workarounds	Coordinates multiparty response Develops advice, workarounds	
PUBLIC AWARENESS	Publishes report	Publishes report	Publishes report	Publishes report	Receives Report
DEPLOYMENT					Deploys fix or mitigation

[2] https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf#page=44&zoom=100,0,309

Appendix no. 2 – Sample Vulnerability Report Form

Vulnerability Report

The information below should be handled as (choose one):

Vulnerability

- Software/Product(s) containing the vulnerability:
- Vulnerability Description:
- How may an attacker exploit this vulnerability? (Proof of Concept);
- What is the impact of exploiting this vulnerability? (What does an attacker gain that the attacker didn't have before?);
- How did you find the vulnerability? (Be specific about tools and versions you used.);
- When did you find the vulnerability?.

Disclosure Plans

- I have already reported this vulnerability to the following vendors and organizations:
- Is this vulnerability being publicly discussed? YES/NO, if yes then provide URL;
- Is there evidence that this vulnerability is being actively exploited? YES/NO, if yes, then provide URL/evidence;
- I plan to publicly disclose this vulnerability:
  - on this date: (Please include your time zone.);
  - at this URL:

Reporter

- Name:
- Organization:
- Email:
- PGP Public Key (ASCII Armored or a URL):
- Telephone:
- May we provide your contact information to third parties? YES/NO
- Do you want to be publicly acknowledged in a disclosure? YES/NO

Additional Information

- Vendor Tracking ID, CERT Tracking ID, or CVE ID if known:
- Additional Comments:

Appendix no. 3 – Sample Vulnerability Disclosure Document

Overview

Brief Vulnerability Description: (1-2 sentences)

Vulnerability ID

- CVE ID for this Vulnerability
- Any other IDs (vendor tracking ID, bug tracker ID, CERT ID, etc.)

Description

- Software/Product(s) containing the vulnerability:
- Version number of vulnerable software/products:
- Product Vendor:
- Type of Vulnerability, if known: (see MITRE's CWE page for list of common types of vulnerabilities)
- Vulnerability Description:
- How may an attacker exploit this vulnerability? (Proof of Concept)

Impact

- What is the impact of exploiting this vulnerability? (What does an attacker gain that the attacker didn't have before?)

CVSS Score

- CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:? – 0.0 (LOW/MEDIUM/HIGH/CRITICAL)
- (Provide the full CVSS vector, not only the score. If possible, provide guidance on the temporal and environmental metrics, not only the base metrics.)

Resolution

- Version containing the fix:
- URL or contact information to obtain the fix:
- Alternately, if no fix is available, list workaround or mitigation advice below.

Reporter

This vulnerability was reported/discovered by _____.

Author and/or Contact Info

For more information or questions, please contact:

- Name:

- Organization:
- Email:
- PGP Public Key (ASCII Armored or a URL)

Disclosure Timeline

- Date of First Vendor Contact Attempt:
- Date of Vendor Response:
- Date of Patch Release:
- Disclosure Date:(List more dates here as necessary to document your communication attempts.)

References

- (List reference URLs here: for example, vendor advisory, other disclosures, and links to advice on mitigating problems.)