Communicating Cybersecurity Vulnerability Information: A Producer-Acquirer Case Study

Hell, Martin; Höst, Martin

Published in:
International Conference on Product-Focused Software Process Improvement

DOI:
10.1007/978-3-030-91452-3_15

2021

Document Version:
Peer reviewed version (aka post-print)

Communicating Cybersecurity Vulnerability Information: A Producer-Acquirer Case Study

Martin Hell[1] and Martin Höst[2]

[1] Lund University, Department of Electrical and Information Technology, Sweden
martin.hell@eit.lth.se
[2] Lund University, Department of Computer Science, Sweden
martin.host@cs.lth.se

Abstract. The increase in both the use of open-source software (OSS) and the number of new vulnerabilities reported in this software constitutes an increased threat to businesses, people, and our society. To mitigate this threat, vulnerability information must be efficiently handled in organizations. In addition, where e.g., IoT devices are integrated into systems, such information must be disseminated from producers, who are implementing patches and new firmware, to acquirers who are responsible for maintaining the systems. We conduct an exploratory case study with one producer of IoT devices and one acquirer of the same devices, where the acquirer integrates the devices into larger systems. Through this two-sided case study, we describe company roles, internal and inter-company communication, and the decisions that need to be made with regard to cybersecurity vulnerabilities. We also identify and discuss both challenges and opportunities for improvements, from the point of view of both the producer and acquirer.

Keywords: Cybersecurity · Open-source software · Case study · Vulnerabilities · IoT

1 Introduction

The use of open-source software (OSS) is increasing and a recent GitHub report shows that for e.g., JavaScript, 94% of active repositories use OSS, with a median number of 10 direct and 683 indirect (or transitive) dependencies [5].

Recently, cybersecurity has made headlines across a range of media. The number of reported vulnerabilities is increasing and cyber attacks are becoming more sophisticated, even with nation-states as the identified attackers [6]. During 2020, the number of new vulnerabilities reported by the National Vulnerability Database (NVD) was more than 18k. This can be compared to the 4-8k annually reported vulnerabilities during 2005-2016 [9].

The combined increase in the use of OSS and the increase in newly found vulnerabilities puts the industry at higher risk than ever. Indeed, OSS vulnerabilities can potentially be exploited in all devices, products, and services that are using those components, though admittedly, just having the component does not

necessarily mean that you are using the vulnerable part [11]. Still, as reported by IBM, scanning for and exploiting vulnerabilities was the top attack vector during 2020, with 35% of all incidents. This is an increase from 30% in 2019 and by that taking over the first position of common attack vectors from phishing [14].

This higher risk raises the bar for how the industry should work with identifying and patching vulnerabilities. However, the producer of devices that are responsible for developing the patches is often not the same as those responsible for maintaining the devices, e.g., installing the new firmware. Moreover, in case of a breach, it is the acquirer that is responsible towards the end customers in the role of delivering and maintaining the system. Thus, in the ecosystem of producers and acquirers, information regarding vulnerabilities and patches needs to be efficiently communicated, such that devices can be immediately updated, reducing the time of exposure [10].

Serror et al. [15] analyze the security aspects of Industrial IoT system ("Industry 4.0") and identify patch management as one important area. Especially for long-lived components procedures for identifying patches are important and for systems with a large number of devices automatic updates are important. There are some attempts to support organizations in vulnerability management through systems for supporting identification, evaluation, and remediation of vulnerabilities [1,2]. To our best knowledge the main focus in research on vulnerability management has been on systems and systems developed by a single organization. There is still a need to understand how communication of vulnerability information between organizations take place, and how the complete processes of managing vulnerabilities can be supported.

Outside the area of vulnerability management there is some research on information sharing between companies. Corallo et al. discusses "Value Networks" and conducts an interview study in an aerospace collaboration with several companies [3]. The focus is on innovation networks, i.e., advanced R&D projects with several partners. They conclude that different activities need different management approaches. Du et al. derive a model for analysing information sharing in supply chains based on game theory [4]. The focus is on supply chains with two parties, and the focus is more on the amount on information sharing rather than the content of the shared information. These aspects are related, but there is still a need to first investigate the actual practices of sharing information about vulnerabilities between organizations and to understand that, before, e.g., more advanced models are built.

The overall goal of this case study is to understand how considerations regarding vulnerabilities in third-party components arise, are communicated, and are assessed within and between a producer and an acquirer. Specifically, through interviews with one producer and one acquirer, we aim to answer the following research questions.

- **RQ1:** What roles and responsibilities can be identified?
- **RQ2:** How is vulnerability information communicated within and between the respective organizations?

– **RQ3:** What decisions must be made and what information is used?
– **RQ4:** What challenges and opportunities can be identified, both within organizations and in the communication between them.

RQ1 is seen as a prerequisite for understanding the organizational context and to adequately understand the result of RQ2. Similarly, RQ3 is used to better understand the challenges and opportunities in RQ4. Based on this, we provide insight into how vulnerabilities in IoT devices are handled on both sides of this producer-acquirer chain, and how they are communicated between the two companies. This insight also allows us to understand what challenges and opportunities there are for improving the handling and the communication of vulnerabilities.

The paper is outlined as follows. In Section 2 we explain the methodology used in our case study, including the involved companies and questions. We also discuss the validity of the research. In Section 3 we give the results, relating to the research questions above. We summarize and discuss the identified challenges and opportunities in Section 4 and we conclude the paper in Section 5.

2 Methodology

The research was conducted as a case study with two companies, a producer and an acquirer. Referring to the case study classifications given in [12,13], we conduct an exploratory case study, meaning that we aim to find out what is happening and seek new insights for the situation where there are questions or issues regarding cybersecurity vulnerabilities. The study is qualitative as it is based on interviews with the involved companies and with a flexible design allowing us to adapt interviews based on the answers from both current and previous interviews. The overall methodology is depicted in Fig. 1. Each company had a company lead for the case study. They had coordinating roles for their respective organization. This coordination included identifying the most suitable people to interview, initiating contact with the interviewees, and continuously discussing the results or possible misconceptions.

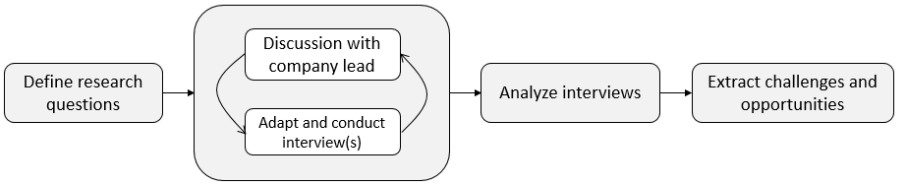

Fig. 1. Overall methodology

Table 1. Participants at companies

Company	Role	Nbr
Producer	Product Specialist	1
Producer	Software Security Group (SSG)	1
Producer	Release Group	1
Producer	First-Line Support	1
Acquirer	Support team technician	2
Acquirer	Head of Support Team	1
Acquirer	Product Owner	1

2.1 Involved Companies

The study focuses on two companies, for confidentiality reasons hereafter called the *producer* and the *acquirer*.

The producer produces and sells products in the area of IoT, primarily in the high-end segment and with a focus on a global B2B market. The IoT units can be seen as embedded systems with hardware and software. The software consists of a combination of in-house developed code and OSS. The organization has a history of more than 30 years, has today more than 1000 employees, and is a leading provider in the high-end segment.

The acquirer has a long tradition of providing high-security systems. It was founded more than 80 years ago and has more than 100 000 employees worldwide. The company has several business units and is active in a wide variety of domains. One core business is to integrate IoT products into larger systems and in turn, being a provider of these systems. The organizational part used in this study provides IoT systems, using products from the producer (among others). The integration of IoT into systems has not been in focus until the last few years. Thus, this specific business is rather new to the company, but knowledge from integrating high-security systems has been transferred also to this business.

Our case study was performed through interviews with representatives from both the producer and the acquirer. The role and affiliation of the interviewees are summarized in Table 1.

2.2 Interview Questions

The interviews were semi-structured, with a set of questions used as a starting point. The research questions RQ1-RQ4 were used as a basis for the questions. For RQ1 (roles and responsibilities), everyone was asked to describe the roles in the organization involved in vulnerability-related questions. This also allowed us to identify additional roles to interview.

For RQ2, we started out with an assumed natural information flow, discussed with and verified by the company leads in the respective organization. The information flow is divided into five steps. In the first three steps, we consider how questions regarding vulnerabilities

1. arise in the acquirers' organization,
2. are communicated to the producer, and
3. are communicated to and from the answering role within the producer's organization.

Once the producer has reached an answer to the question, this answer is returned to the acquirer. The parts related to the answer are divided into

4. how the answer is communicated back to the acquirer, and
5. how the answer is communicated within the acquiring organization.

The sequence of events starts at (1) in case the question is sent to the producer, but it can also be initiated at (4) in case of publishing advisories or if the producer pre-emptively contacts the acquirer with information.

For the acquirer, this was from the point of view of questions only targeting this particular producer, but for the producer, the scope was vulnerability-related questions from all their customers. In addition to the information flow, we also aimed to understand who is making the decisions, and what information was used to make decisions (RQ3). These questions were integrated with (3) and (4) above for the producer, and (5) for the acquirer, as this became a natural part of the interviews. The final part of the interviews was devoted to identifying possible improvements to the different parts of this process (RQ4). Improvements are here defined as initiatives or modifications that could make this process either easier for the involved people, more efficient for the organization, or more accurate in terms of providing answers to questions.

Since the interviewees had different roles in the information chain, the focus of the questions varied somewhat. Understanding the overall information and role structure was our first objective, achieved together with the company leads (and verified during interviews). Then, the interview focus could be tailored for that role in the information chain.

A last thing to note is that the interviews were also adopted to allow us to verify claims and descriptions from previous interviews.

2.3 Validity

The validity of the research has been considered during the planning through a number of measures.

- *Prolonged involvement* means that the research is not conducted in isolation, meaning that there is a trust between parties. In this case, the study was conducted in a setting with a longer cooperation, and the coordinators have cooperated with the researchers in other studies.
- *Triangulation* was mainly achieved in the interviews by repeating questions and checking results with several roles in the two organizations.
- *Peer debriefing* means that a group of researchers were involved and thereby the risk of bias from one researcher is avoided. In this case, both authors were involved in discussions and interpretation of the results.

– *Member checking* means that, e.g., participants in the study review and reflect on the results. In this case, especially the coordinators were involved during the study e.g. available to answer questions about results and helping out to interpret results.
– *Audit trail* means keeping track of all data in a systematic way. In this study, notes were taken from all interviews, and the analysis was based on these notes. The researcher that took the notes was the main person in the analysis which solves the main problems of interpreting notes from someone else.

Based on the methodology and these measures our view is that the main validity problem is external validity. Care must be taken when generalizing the results, but we believe that the findings can still serve as input to further studies.

3 Results

In this section, we present the results from our interviews. Each subsection corresponds to one of the research questions presented in Section 1.

3.1 Roles and Responsibilities

The acquirer has responsibility for the actual products and their integration into the operating environments. Attacks taking advantage of vulnerabilities in the products will in the end affect their customers so vulnerability information is essential for securing customers' environments and assets. Vulnerabilities are typically handled by updating or patching the firmware. Since this can be associated with large costs it is important to understand the impact of the vulnerabilities. Recall that the acquirer organizational part in focus in this study manages units at their customers' sites. We have identified the following roles and responsibilities within this organizational part for handling vulnerabilities.

– The *support team* is centralized in one country and provides a "managed by" solution to the production teams. It consists of approximately 20 people, including both technicians, management, and sales. The support team introduces new functionality and is responsible for identifying and prioritizing new vulnerabilities found in the products. They are not in contact with the actual customer sites.
– Each country has one *production team*, offering the integrated system to end customers. When new vulnerabilities are discovered, they are responsible for communicating with their customers, and also to deploy new firmware to the individual units.
– The *product owner* defines the requirements for the "managed by" product. This role does not take an active part in the process and is not part of the actual decision regarding vulnerabilities.

The producer, being a provider of high-end products, is working with security in a structured way. The organization takes inspiration from the BSIMM maturity model [7], with a core software security group that has close contact with

development teams. Much effort is put into raising awareness throughout the organizations using so-called satellites, people with interest in security that can help to disseminate knowledge and information to their respective teams. For vulnerabilities in third-party components specifically, we identify the following roles and responsibilities.

- *First line support* receives security-related questions from customers. Here we also include key account managers, though these are formally part of the sales organizations. First-line support either answers the questions directly or forward them to a product specialist, while the key account manager opens a support issue with first-line support in order to make sure that all questions pass their organization and expertise.
- The *product specialists* have deep knowledge about the products and take an active part in product development and sprint planning. They have thus direct contact with developers. They are responsible for answering questions that can not be immediately answered by first-line support.
- The *development teams* are responsible for integrating OSS components. Individual developers are also responsible for keeping track of the OSS components and monitoring new updates, features, and vulnerabilities.
- The *software security group* (SSG) develops and leads the security initiatives throughout the company. They are experts in the technical details surrounding vulnerabilities. They are responsible for conducting the triage of new vulnerabilities, i.e., understanding the exploitability and impact of vulnerabilities in the context of the products and their operating environment.
- The *release team* is responsible for making new firmware releases in case of newly discovered vulnerabilities require immediate patching. New firmware can be released the same day if needed, provided that the developers have implemented the patch. The main bottleneck is often to identify which devices need new firmware.

These roles were agreed upon by all participants in this study.

3.2 Communication Within and Between Producer and Acquirer

How Questions Arise Within the Acquirer's Organization Product and software security is the responsibility of the support team. The roles and the communication paths for security vulnerabilities are depicted in Fig. 2. Note that the different production teams typically do not communicate with each other at all. While questions potentially could arise directly from customers, through the production team, and to the support team, this has so far not happened. Since the customer purchases a solution, they typically assume that vulnerabilities are handled by the acquirer. A similar assumption is made by the production team, namely that since the support team is responsible for security, those issues are handled by them. The support team has two main sources of vulnerability-related information that can lead to questions escalating to the producer.

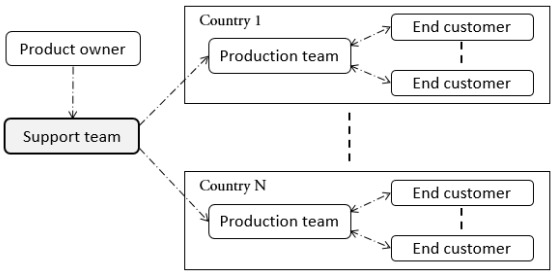

Fig. 2. Virtually all vulnerability related questions stems from and are handled by the support team.

- *Externally produced information material.* This mainly includes forum discussions, news articles, and research articles.
- *Internally produced information material.* This material is dominated by reports from vulnerability scans.

Of these two, the latter is most common. The support team regularly scans the network, searching for units and possible vulnerabilities in these. This is done on a weekly basis for central parts of the systems, but for other parts, it is much less regular. Finding information from externally produced material is much less formalized. Searches are at best done on an ad-hoc basis, and most information reaches the teams due to wide media coverage.

How Questions are Communicated to the Producer During the interviews, both the producer and acquirer were asked about how, what, and to/from whom questions were communicated. A summary of the answers is given in Table 2. Note that the producer referred to questions from all its customers, not only the specific acquirer in this study.

An interesting observation is that the producer organization often does not know the role or background of the one asking. First-line support, receiving the original question, had the impression that it was not security experts, but mostly junior with little or no security training.

> "It is very rare that the question comes from someone with deep cybersecurity knowledge or even someone in the cybersecurity business. It is rather someone that just got the task to run a network scan on the equipment."

Since the actual role is unclear, this information is not propagated in the organization together with the question. This is a limiting factor since the technical level of the response can then not be aligned with the person asking the question. While the SSG expressed some concerns about this in the interview, the product specialists never experienced any actual problems related to this. Answers were always accepted as is.

Table 2. A summary of how vulnerability related questions are communicated to the producer, both from the producer and acquirer's point of view.

Questions	Answers
Who is asking the question?	**Producer:** Not clear, but seems to not be security experts. **Acquirer:** Support technicians (through a web portal) or head of support team (to key account manager). The latter is most common.
Who is the question directed towards?	**Producer:** First line support gets basically all questions, but sometimes through the key account manager. **Acquirer:** Key account manager directly, or using support portal in which case recipient is unknown.
What question medium is used?	**Producer:** Always through a webform, ending up in the CRM. A support email address is not even provided. **Acquirer:** Mostly through a web form but sometimes phone calls to key account manager.
What do the customers want to know?	**Producer:** One or more of "Do you know about this vulnerability?", "How did you handle it?", "Is it fixed?", "Can we protect us in ways other than patching?". **Acquirer:** Are we affected by this vulnerability?
How is the question posed?	**Producer:** By submitting a list of CVE numbers or vulnerability scanning results. **Acquirer:** If they are affected by a specific vulnerability, referring to a vulnerability scan or CVE number.
How often do you get/ask questions about vulnerabilities?	**Producer:** 1-2 per month for first-line support in one country, 3 per week to PS (from all first-line support units), 1 per month to SSG **Acquirer:** Several times per year, but not as often as once per month.

The producer observed that a very common event is that (information from) a report from vulnerability scanning is sent to the producer, with the goal of understanding to which extent deployed units are vulnerable. The information can be in the form of a report or a screenshot from the scanner, with the accompanying question "We seem to have these vulnerabilities, is it true and how do we fix it?"

This description fits very well with how this was actually done at the acquirer side, with regular network scans to identify problems and vulnerabilities.

All questions are directed to first-line support. This is the main channel for customer support. Customers send their questions through the online helpdesk portal, while some have a direct connection to a key account manager and send their questions directly to them, either by phone or by email. For security-related questions, the key account manager must always open an issue with first-line

support such that these questions go through them. This is nowadays strictly enforced due to historical events where bypassing first-line support resulted in delays and misinformation.

Not only do many questions arise from vulnerability scans, but the results of these scans are often directly referenced in the question. Many customers use consultants for security and penetration testing, which results in a list of potential vulnerabilities. Since the customers do not have the expertise to interpret and validate the results of such scans, and it is not clear if the products are really affected, such scans escalate to questions directly to the producer.

For one first-line support country, the number of vulnerability-related questions are in the order of a few per month. This amounts to a very small proportion of the total number of questions ($< 1\%$), but it was still evident that the numbers have increased over the last few years.

On very rare occasions, the customer asks for a meeting with the R&D department. This can happen when they are afraid that the problem is serious, and they require firsthand and immediate information on how to take action.

Communication to Answering Role within Producer's Organization The communication inside the producer's organization is depicted in Fig. 3. As noted in Section 3.2, questions are directed to first-line support, or possibly to the key account manager who in turn forwards it to first-line support. Sometimes, first-line support can answer directly, but if this is not the case, security-related questions are re-directed to the product specialists, since the questions are related to the products. It was estimated that 70% of all questions were answered directly by first-line support, and 30% propagated further. For these 70%, it was almost always the case that an old firmware version was used and the solution was to update to the newest firmware.

Upon reaching the product specialist, these can sometimes answer the question directly. This primarily happens if the question has been asked before, or if the answer can be found from previous security-related discussions. A quick search in the email inbox can often answer this. Otherwise, if the question is related to a CVE identifier, then the NVD database is used to find more information. This database includes a short description of the vulnerability, a severity score (CVSS), information on vulnerable and non-vulnerable versions, and links to further information about the vulnerability. While it has been shown that this information is not always accurate [8], it can still provide enough information to answer the question, e.g., in which version the vulnerability was patched. The product specialist then contacts the development team to see when the software was patched. Questions stemming from external media are often related to new vulnerabilities, which are not patched in deployed releases. The product specialist works closely with the development teams and takes part in sprint planning and prioritization of tickets. Thus, they have a direct connection to finding out when software is patched.

It should be noted that the time of patching is not the same as releasing a new firmware. The answer the product specialist is really looking for is when

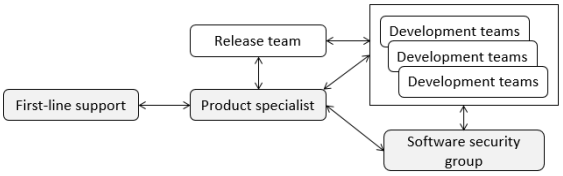

Fig. 3. First-line support, product specialists, and the software security group handle vulnerability related questions. Development teams implement patches and the release team compiles the new firmware.

the new release appears, not when it was patched on the main branch. This is controlled by a release team, which communicates closely with the developers and the product specialist in case there are severe vulnerabilities that must be fixed. If needed a new secure firmware can be released within a day. However, in most cases, this team is not aware of the fact that the new release includes particular vulnerability fixes. The release notes, which include vulnerability information, are written by the product specialist.

The software security group is sometimes involved in the process. This is typically when the vulnerabilities require additional effort for "triaging" and to understand their potential impact. Some technical details of a vulnerability can often be very involved, in which case the product specialist can not answer directly. SSG is the last resort for answering questions. At this stage, the product specialist has refined the question, from the result of a vulnerability scan to a more direct question related to a CVE. For a CVE, the SSG performs a triage process, which is further discussed in Section 3.3. SSG has no communication with first-line support at all.

Communication Back to Acquirer When an answer has been found to an explicit question, it is communicated back to the acquirer through email, or specifically in the CRM which results in an email to the registered address. Communication is always through first-line support. If the question escalated all the way to SSG, then it is returned to first-line support through the product specialist.

Some questions are implicitly answered by release notes and advisories. Release notes describe what has been changed for a specific release and which vulnerabilities, if any, have been solved. The advisory is a specific document, often relating to one or a few vulnerabilities of particular importance. The document can provide information on both workarounds and/or which firmware release to upgrade to. Advisories can be a result of questions, but can also be initiated directly from the producer's organization as a pre-emptive measure, acknowledging that many customers will benefit from this information. The release notes are written by the product specialist.

A third possibility is that the key account manager directly contacts the acquirer. This is often the case for important vulnerabilities, where the producer quickly wants to disseminate the information to the largest customers. This is an example of communication originating on the producer's side, i.e., starting with step (4) as given in Section 2.2.

How Answers are Communicated within the Acquiring Organization. Answers are returned to the support team via email. This email initiates an immediate meeting, where the answer is discussed. The following aspects are discussed at this meeting.

- To which extent does the vulnerability affect the organization and its customers?
- What is required to fix the problem (amount of work)?
- Can the support team fix this or is production team involvement needed?
- How urgent is it?
- What preparation is needed by the support team?

Based on this information, the head of the support team contacts the affected production teams, who in turn are responsible for upgrading the firmware to a non-vulnerable version. There is no follow-up that the new firmware has actually been installed, mostly because there are no technical tools for doing this. Thus, this can be seen as a one-way communication of the information from the support team to the production teams.

3.3 Decision and Information

To answer the question if a customer's product is vulnerable to a given vulnerability, several pieces of information are needed

- Product information. This includes the type of product(s) and the firmware version(s) used.
- Vulnerability information. This includes which versions of the software are vulnerable and which are not.

As the majority of vulnerability-related questions are posed in the form of a vulnerability scan report, such reports typically include the vulnerability identifier. Most often the model identifier is also included when the question is sent, but it happens that a follow-up question is needed to identify this.

Knowing the product and model, first-line support looks at the release notes which very often enumerate which vulnerabilities have been remedied in a specific firmware. Most of the time the vulnerability is listed in release notes and the answer to upgrade and to which firmware version can be delivered promptly. First-line support has a Service-Level Agreement (SLA) with a defined number of hours for answering questions, but vulnerability-related issues are prioritized and the answer is often returned within a few hours depending on the issue

queue and office hours. Handling a specific vulnerability-related question is often finished in around 30 minutes upon opening the issue.

Further vulnerability information is typically found in NVD. First-line support does not go this far in their analysis, but this is a primary information source for the product specialist. Together with the development teams, this information can reveal which firmware releases could be vulnerable.

Having a vulnerable version does not equal being vulnerable. Additional work on understanding vulnerabilities is performed by SSG in a vulnerability triage process. This process includes looking at the base CVSS score for a vulnerability and understand how it affects the products. Sometimes high severity vulnerabilities turn out to be of very low or no severity in the product. This is e.g., the case if the vulnerable part of a component is not even used by the product. Other times, but less often, low severity vulnerabilities turn out to be of higher severity in the product. One example could be if availability impact is low, but considered of very high importance to the product. A full severity analysis can however not be performed since the SSG only knows how the software is used in the product, but not how the product is used in an actual system.

The acquirer instead has the information needed to decide if they are actually vulnerable. As one example, in the systems that they manage, the devices are typically not reachable from the public Internet but resides on their own networks. This can dramatically affect the exploitability of the vulnerability and how to prioritize an update. Such contextualized information is not known to the producer. It is clear that the information gathering and decisions are here very centralized to the support team.

3.4 Identified Challenges and Opportunities

In this section, we discuss challenges and opportunities that were identified in our interviews.

From the Producer's Point of View As noted in Section 3.2, the vulnerability scanning performed by the acquirer is often used as a basis for questions. They wish to better understand if they are vulnerable. At the same time, the producer also performs similar vulnerability scanning of their products. Using results from these scans could be used to more efficiently answer such questions, but a process to leverage this has not been defined.

The escalation of questions from first-line support, to the product specialist, and finally to SSG heavily relies on either searching in email correspondence or using the collective memory of the product specialists. Both the product specialist and the SSG representative identified this as a possible area of improvement.

> "This system could break when the company grows or with growing employee turnover."

A better approach would be to document relevant information. Moreover, the vast majority of vulnerabilities are already known to the SSG or to develop-

ers, being responsible for that OSS, so the information flow can be made more efficient by documenting this analysis and vulnerability information.

A possible improvement for first-line support would be to have more security training. They do have access to a set of training videos, but many questions come in as scanning reports, and one suggestion was to let the people working in first-line support do such scanning themselves, just to get an idea of how they work and the information they provide. Submitted reports sometimes lead to a bit of "panic" and with more understanding, they could carry out their investigation with more confidence. There is currently one person with security training and OSCP certification, who often becomes the go-to person for all these issues.

From the Acquirer's Point of View Though vulnerability scans against deployed products are performed on a regular basis, there is no structured work for security vulnerabilities. This includes monitoring information sources for faster identification of potential vulnerabilities. At the same time, there is much trust in the producer's ability to fix vulnerabilities and it is convenient to leave this responsibility to the producer. There are also no recorded events of when things have gone wrong. Still, there is a perceived need to have a more structured approach to security and vulnerabilities. To this extent, the information provided by the producer, both in release notes and in answers to direct questions is often not enough to make informed decisions.

4 Discussion & Analysis

Based on the results in Section 3, we summarize a set of challenges and opportunities that have been identified.

Challenge: *Scattered knowledge.*
There is little or no centralization of knowledge regarding vulnerabilities within the producer's organization. The knowledge is built and disseminated by different parts of the organization, while at the same time being information that needs to be communicated quickly in order to protect the managed systems from attacks. While having a well-defined process for handling vulnerability-related questions from customers, this decentralization of knowledge could have a negative effect on efficiency and accuracy in case there is a higher turnover of employees in the future.
Challenge: *Role-targeted security training.*
Though first-line support answers a majority of vulnerability-related questions, they lack security training, and in particular training targeting the actual questions that they receive. This lowers their confidence when it comes to these types of questions.
Challenge: *Strong reliance on the producer.*
The acquirer is strongly reliant on the producer providing firmware updates and

timely information. Much information regarding vulnerabilities in devices is provided through release notes. With many devices and models, it is hard to track the newly released firmware and understand which needs to be applied urgently and which can wait until regular maintenance.

Opportunity: *Leverage internal scan information.*
Re-using and centralizing information from internal scans can increase the understanding of customers' challenges. Since there is in-house scanning of firmware already in place, transferring this knowledge to first-line support seems to be a cost-efficient way of increasing efficiency, accuracy, and confidence in answering questions.

Opportunity: *Register for Release Notes.* Release notes are linked to a specific firmware, and the firmware is only applicable to a set of device types and models. Allowing the acquirer to subscribe to release notes for certain devices and models can help them to more efficiently identify if the vulnerability applies to them or not. This need was described by the acquirer, and based on the fact that many answers are found by first-line support consulting the release notes, this could potentially also reduce the number of support cases.

The fact that the answer often is not enough to make decisions is reasonable. Indeed, the producer has no knowledge of the environment in which the products are operating. Vulnerability information is often generic, and it is up to the affected party to determine to which extent the vulnerability can be exploited. Only to some extent, this can be done by the triage at the producer's side since they know how the software is used in the product. This is also evident in the severity score given to vulnerabilities (CVSS), where the worst-case scenario is assumed when determining the base score. The environmental CVSS score is instead defined for adjusting the severity level for the operating environment. This highlights the need for security expertise throughout the supply chain.

5 Conclusion

We conducted a case study to better understand how vulnerability-related questions are handled by a producer and an acquirer of IoT devices. We describe both how such questions are handled in the respective company and how the information is communicated between them. The study is motivated by the fact that the use of OSS is increasing and that new vulnerabilities are discovered and reported to public databases at an increasing rate. Having an efficient process for identifying, analyzing, and communicating information regarding firmware upgrades is essential to mitigate an increased cybersecurity threat. Our study revealed a set of challenges and opportunities that can be considered to facilitate improved processes. While these are identified based on the involved companies' needs and procedures, we believe that they can also be considered by other companies to improve their cybersecurity. For future work, it would be valuable to better understand if, how and why vulnerability-related information fundamentally differs from other types of time-critical information that need to be communicated within or between organizations. Such an understanding could allow us to

identify optimizations, both from a technical, but also from an organizational perspective.

Acknowledgements This research was funded in part by the Swedish Government Agency for Innovation Systems (Vinnova), grant 2018-03965, and in part by the Swedish Foundation for Strategic Research, grant RIT17-0035.

References

1. Aldea, M., Gheorghică, D., Croitoru, V.: Software vulnerabilities integrated management system. In: proceedings 13th International Conference on Communications (COMM). pp. 97–102 (2020)
2. Cobleigh, A., Hell, M., Karlsson, L., Reimer, O., Sönnerup, J., Wisenhoff, D.: Identifying, prioritizing and evaluating vulnerabilities in third party code. In: 2018 IEEE 22nd International Enterprise Distributed Object Computing Workshop (EDOCW). pp. 208–211 (2018)
3. Corallo, A., Lazoi, M.: Value network collaborations for innovations in an aerospace company. In: proceedings IEEE International Technology Management Conference (ICE) (2010)
4. Du, Z.T., Xie, X.Z.: Research on construction strategy of enterprise information sharing in supply chain. In: proceedings International Conference of Information Science and Management Engineering (ISME). pp. 49–53 (2010)
5. GitHub: The 2020 state of the octoverse. `https://octoverse.github.com` (2020)
6. Mansfield-Devine, S.: Nation-state attacks: the escalating menace. Network Security **2020**(12), 12–17 (2020)
7. Migues, S., Steven, J., Ware, M.: Building security in maturity model – version 11. `https://www.bsimm.com` (2021)
8. Nguyen, V.H., Massacci, F.: The (un)reliability of NVD vulnerable versions data: An empirical experiment on google chrome vulnerabilities. In: proceedings 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. pp. 493–498 (2013)
9. NIST: National vulnerability database. `https://nvd.nist.gov/` (2021)
10. Olsson, T., Hell, M., Höst, M., Franke, U., Borg, M.: Sharing of vulnerability information among companies – a survey of swedish companies. In: proceedings Euromicro Conference on Software Engineering and Advanced Applications (SEAA). pp. 284–291 (2019). https://doi.org/10.1109/SEAA.2019.00051
11. Ponta, S.E., Plate, H., Sabetta, A.: Beyond metadata: Code-centric and usage-based analysis of known vulnerabilities in open-source software. In: proceedings IEEE International Conference on Software Maintenance and Evolution (ICSME) (2018)
12. Robson, C.: Real World Research: A Resource for Social Scientists and Practisioner-Researchers. Blackwell (2002)
13. Runeson, P., Höst, M., Rainer, A., Regnell, B.: Case Study Research in Software Engineering - Guidelines and Examples. Wiley (2012)
14. Security, I.: X-force threat intelligence index 2021. `https://www.ibm.com/se-en/security/data-breach/threat-intelligence` (2021)
15. Serror, M., Hack, S., Henze, M., Schuba, M., Wehrle, K.: Challenges and opportunities in securing the industrial internet of things. IEEE Transactions on Industrial Informatics **17**(5), 2985–2996 (2021). https://doi.org/10.1109/TII.2020.3023507