Federal Office
for Information Security

RECOMMENDATION: IT-PRODUCERS

Vulnerability Handling

Recommendations for software vendors

In the vendor's view, providing information on vulnerabilities in software components might be perceived as an indication for insufficient quality and thus might cause loss in sales. Therefore the principle of 'security by obscurity' is widely followed, i.e. no or only inadequate information on even serious vulnerabilities is published. It is just this way of thinking that can lead to situations where attackers already have detailed knowledge on these vulnerabilities by own research or by buying it from experts. Those attackers might then exploit these vulnerabilities and the asset owners remain as those who are affected from the resulting damage. Furthermore, third parties don't always follow the principle of 'coordinated disclosure' (also referred to as 'responsible disclosure') when publishing information on vulnerabilities. 'Coordinated' means that a vulnerability is reported confidentially. The researcher who discovered it cooperates with the vendor to develop a proper update and information on the vulnerability is disseminated after remediation of the threat. The reason for not acting according to 'coordinated disclosure' is that vendors often don't offer sufficient ways to be contacted or they don't respond after an initial contacting.

This document gives recommendations for vendors of software products and other IT products involving some kind of firmware on the proper handling of vulnerabilities. This includes internal preparation, setting up communication channels, the actual incident handling and the post-processing phase. Vendors following these recommendations may distinguish from competing companies which can result in increased customer satisfaction and company benefit.

In addition to these recommendations, the BSI analysis on cyber security 'Life-cycle of a vulnerability'[1] lays out the basics on vulnerabilities in general and principles such as 'coordinated disclosure' and 'full disclosure'.

Internal preparation

A vendor should make sure to be prepared to handle an incident even before a vulnerability in a product is discovered. First of all, the handling of vulnerabilities has to be managed within the company. This especially includes:

- Disclosure policy
- Roles and entitlements (Who does / decides what?).
- Internal processes including time limits (response time) which cover the reproduction and understanding of the vulnerability, elaboration of workarounds and development and testing of patches.
- The awareness that a professional handling of product vulnerabilities with respect to both customers and discoverers is required.

The 'disclosure policy' or 'vulnerability handling policy' is a guideline that defines how a vendor deals with vulnerabilities. It is very important as it helps building confidence between the vendor

[1] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/OffenerBereich/Sensibilisierung/sensibilisierung_node.html

and a researcher. The main purpose of such a policy is to give detailed information on how the vendor defines or interprets the term 'coordinated disclosure' and what that means for a security researcher. This should include a statement of practice on how the vendor will handle the researcher's data with regards to confidentiality, potential public disclosure and what is expected from the researcher. There should also be detailed information on how the processes employed by the vendor influence the fixing of a vulnerability and what this implies for the researcher. For instance, the vendor may expect the researcher to withhold any kind of publications on the vulnerability at conferences or in the media.

In order not to scare researchers, the vendor should not demand formal or legal agreements such as contracts, a formal Memorandum of Understanding (MoU) or a Non-Disclosure Agreement (NDA). Especially, the vendor should point out that researchers will not be sued at least as long as they stick to the ground rules laid out by the vendor.

Furthermore, the disclosure policy should tell the researcher what he can expect from the vendor. Therefore it should include information on reward programs (bug bounties) available which reward for the discovery of a vulnerability and for following the principle of coordinated disclosure.

Communication channels

Establishing proper communication channels between the vendor on the one hand and customers and security researchers on the other hand is essential in order to act efficient and short-term in case of a vulnerability. In general it is recommended not to entitle single employees as a point of contact for security issues since for instance employee turnover may cause problems. Rather than that, points of contact shall be role based and made available on the company's website as well as in the product documentation.

The vendor's website

As primary communication channels, the company's website, email and phone are recommended. Information on communication channels regarding security issues should already be included on the index of the company's website.

A vendor's website shall offer security related information at a central position. This includes general security information (e. g. https://www.company.tld/security) as well as security related information specific to certain products. Depending on the complexity of the product portfolio this can be offered on a separate web page such as https://www.company.tld/productname/security. The usage of SSL should be mandatory here.

Such a security related web page should contain:

- vulnerability information (advisories on vulnerabilities not fixed yet, information regarding possible workarounds and bulletins on vulnerabilities for which security updates are available).
- Contact information specific for security of products (email, phone including services hours, public PGP keys and S/MIME certificates of the company to enable confidential communication on security issues).
- The company's disclosure policy.
- Patches and updates.
- Supplemental documents (whitepapers, FAQ, etc.) regarding the secure usage of products.
- A contact form which allows the vendor to structure the information flow and to make certain information mandatory. In addition such a form supports the alternative to report vulnerabilities anonymously. The company should decide if such a form is relatively simple (e.g. Ebay[2]) or more complex (e. g. cert.org[3]).

These web pages shall be protected using valid and verifiable SSL certificates to guarantee authenticity and confidentiality of the information provided.

As a central email address for security related questions and reports it is recommended to use addresses

[2] http://pages.ebay.com/securitycenter/Researchers.html

[3] https://forms.cert.org/VulReport/

such as product-security@company.tld, security-team@company.tld, productname.security@company.tld or secure@company.tld. Security@company.tld should not be used since according to RFC 2142 this address has a different purpose. Likewise, common addresses such as info@company.tld or support@company.tld should not be used for security related issues. It is essential to provide valid S/MIME certificates and PGP keys to assure authentic and confidential communication.

Security related questions or reports via the communication channels offered by the vendor should be answered during 24 hours (1st level) with a personal email that is not automatically generated. After a more detailed analysis (2nd or 3rd level), there should be an additional information within another 48 or 72 hours.

Vendors should offer mailing lists for security related information. The emails delivered to these lists should be protected by digital signatures using the same keys and certificates that are published on the vendor's website.

Especially in critical fields of application, publicly available information on security related vulnerabilities can be very dangerous. In this case the asset owners, OEM partners and other customers affected should be informed directly.

In addition to the vendor's website there are several lists on the internet where vendors can publish their contact information, such as

- http://osvdb.org/vendors
- http://oss-security.openwall.org/wiki/vendors
- http://ocert.org/team_and_members.html

Networking with third parties

It is recommended to maintain a network to third parties in order to react short-term, especially when a vulnerability has exceptional impact. This may include contacts to governmental institutions such as the BSI, industrial associations and CERTs in other countries. Especially for products with significance to critical infrastructures (German KRITIS, US CIKR), an institution such as the BSI can aid in disseminating the information. Therefore it is helpful to have detailed information on the countries, industries and scenarios in which the affected product is used. Furthermore, registering to a CERT enables a vendor to get the latest advisories and warnings on products that affect his products and his own infrastructure. It is also useful to keep in contact with business competitors, partners and other institutions such as industry forums and testing laboratories.

Particularly with regards to vulnerabilities that arise from problems of major vendors or common protocols and technologies it is very important to exchange within the industry. Especially third party code such as frameworks and libraries should be given special consideration when it comes to security. By using such third party components they become part of the own product. Therefore a security contact should be established to each vendor of such components and their advisories should be checked at least on a daily basis. Advisories or bulletins of third parties should be followed by appropriate actions. This includes measures such backporting patches, upgrading components and issuing advisories.

There might be situations where it turns out the root cause for a reported vulnerability is within a third party component. This should be communicated to the affected vendor as soon as possible. Each of the affected parties should act in a constructive manner to solve such a complex issue. The same constructive and open efforts should be made when other vendors are affected by a vulnerability in an own product.

Handling the issue

The most important tools for external communications during (if possible short-term) vulnerability handling are advisories and bulletins.

An advisory shall contain the following:

- title or identifier of the advisory (e. g. systematically and consecutively numbered)
- date of publication
- affected products, versions and configurations
- affected platforms and operating systems (and where appropriate their configuration)
- criticality (categorization low/medium/high) and estimation according to the Common Vulnerability Scoring System (CVSS)[4]
- implications (e. g. denial of service, remote code execution, local privilege escalation, etc.)
- short description of the vulnerability (Management Summary)
- detailed description (for technical staff)
- estimated availability of patch/update
- history / timeline regarding events relevant to this vulnerability
- workarounds
- appreciation of the discoverers
- information of the way the vulnerability was reported/published (e. g. coordinated disclosure)
- information whether exploit or proof-of-concept code is publicly available
- authors of the advisory
- CVE Number or CVE Candidate Reference Number[5].
- Supplemental information
- URL to the up-to-date version of the advisory

If an advisory is updated, the additional or modified sections should be clearly marked as an update.

An advisory should not include any information that allows technically skilled experts to exploit the vulnerability. Also exploit code (proof of concept code) to illustrate the vulnerability or to check whether a system is affected should not be published since it could be abused immediately.

Advisories should be signed with the same cryptographic keys that are available on the company's web page. The advisory should include a URL to that page.

As soon as a security update / patch is available, the advisory is turned into a bulletin that includes further information on the security update for the affected products. This includes information on where to get the update, possible incompatibilities and alternative protective measures in case it is not possible to deploy the security update.

Both advisories and bulletins should be published as soon as possible, but generally accuracy should not be neglected due to timeliness.

The aftermath

After finishing vulnerability handling there should be a wrap-up to conclude the lessons learned. For instance, it might be necessary to improve communication behavior or the processes of vulnerability handling. Another lessons learned is to identify possible improvements in the development process and quality management of the product. This might include establishing quality gates or additional test methods and test patterns. In general the development of IT components should follow an established development methodology which addresses security in a sufficient manner.

In the BSI-Publications on Cyber-Security, the Federal Office for Information Security (BSI) releases proposals and recommendations on current topics concerning Cyber-Security. The contents are researched and compiled with best accuracy and in all conscience. If you have any comments or information, please contact: cs-info@bsi.bund.de.

[4] http://www.first.org/cvss

[5] http://cve.mitre.org