IoT Security Foundation - IoT Security Foundation - IoT Security Foundation

BEST PRACTICE USER ✓

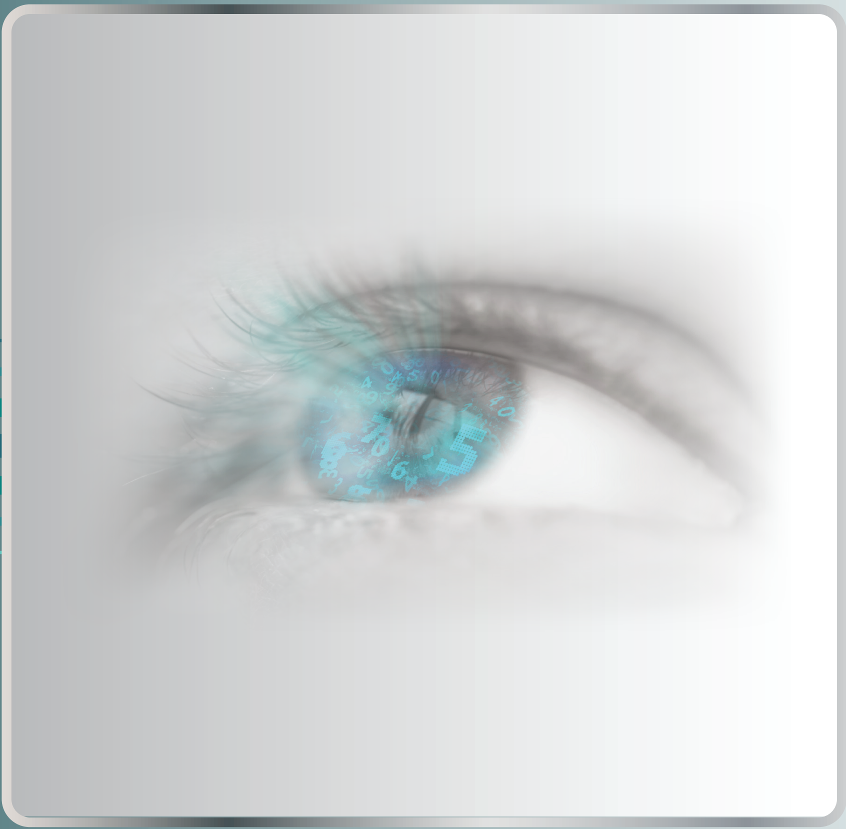
© IoTSF 2016

IoT Security Foundation

Vulnerability Disclosure

Release 1.1, December 2017

Best Practice Guidelines



Notices, Disclaimer, Terms of Use, Copyright and Trade Marks and Licensing

Notices

Documents published by the IoT Security Foundation ("IoTSF") are subject to regular review and may be updated or subject to change at any time. The current status of IoTSF publications, including this document, can be seen on the public website at: https://iotsecurityfoundation.org/

Terms of Use

The role of IoTSF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.

In making this document available, no provision of service is constituted or rendered by IoTSF to any recipient or user of this document or to any third party.

Disclaimer

IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.

IoTSF is a non-profit organisation which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF's membership and partners. IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high quality guidance, IoTSF provides all materials (including this document) solely on an 'as is' basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation.

By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Copyright, Trade Marks and Licensing

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members and external reviewers.

- Steve Babbage, Vodafone Group Plc
- Craig Heath, Franklin Heath Ltd
- John Haine, University of Bristol
- Richard Marshall, Xitex Ltd
- John Moor, IoT Security Foundation
- Kenny Paterson, Royal Holloway of London
- David Rogers, Copper Horse Solutions Ltd

Contents

1 Introduction

1.1 Overview

Vulnerability disclosure is an increasingly important topic, especially for providers of Internet-of-Things (IoT) products and solutions. To avoid unnecessary risk to both the providers and users of these offerings when security issues are found by external parties, providers should set expectations of a clear process for responding to reports of such issues and for managing the public disclosure of information regarding them. The process should cover both the reporting of newly discovered security vulnerabilities to the product- or service-providing organisation and the public announcement of security vulnerabilities by that organisation (usually following the release of a software patch, hardware fix, or other remediation).

This document provides manufacturers, integrators, distributors and retailers of IoT products and services with a set of guidelines for handling the disclosure of security vulnerabilities, based on best practice and international standards. The IoT Security Foundation are also developing a companion document to be released in early 2018, *Introduction to Vulnerability Disclosure in the Internet of Things*, which introduces the concepts and discusses the advantages of managing vulnerability disclosure in a standardised way.

1.2 Scope

This document presents best practice guidelines for a vulnerability disclosure process, targeted for adoption by IoT solution providers, device vendors and service providers. The recommended process is described by reference to the international standard ISO/IEC 29147:2014, *Information technology -- Security techniques -- Vulnerability disclosure*,[ISO2014] the electronic version of which may be downloaded free of charge from the following URL:

http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

Please note that this document does not address the management of any data breach which may have resulted from the exploitation of a security vulnerability; an organisation's responsibilities regarding this are usually determined by applicable legislation and government regulations, particularly regarding individuals' personal data, in the territories and/or industry sectors in which they operate. You should ensure that your organisation is fully aware of, and in compliance with, any data protection requirements which may apply.

2 Vulnerability Disclosure Process Guidelines

It is up to each individual provider to decide exactly what process to adopt, but it is important to be clear about the process in public materials, websites and in communications with researchers in order to align expectations. It can also be beneficial to have a certain amount of flexibility in certain cases.

Alternative types of disclosure process will be discussed in our companion introductory material. For typical use, we are describing what is called there a "Coordinated Vulnerability Disclosure" process, as being the most equitable and reasonable.

2.1 Website

It is essential that security researchers can be channelled to the right point of contact within the provider organisation, so it is imperative that there is an easy-to-find web page which contains all the necessary information. It is recommended that the address: http://www.companydomain/security is used, so for the IoT Security Foundation this is: http://www.iotsecurityfoundation.org/security. It is also recommended that the organisation's 'Contact' page contains a referring link to the Security page.

2.2 Sample Web Page Text

The following is some proposed text for inclusion on a Vulnerability Disclosure page on a company website, to be approved by the company's legal team. Some companies also choose to specify what they consider to be unacceptable security research (such as that which would lead to the disclosure of customer data):

> *"[Company Name] takes security issues extremely seriously and welcomes feedback from security researchers in order to improve the security of its*

products and services. We operate a policy of coordinated disclosure for dealing with reports of security vulnerabilities and issues.

To privately report a suspected security issue to us, please send an email to security alert@<companydomain>, giving as much detail as you can. We will respond to you as soon as possible. If the suspected security issue is confirmed, we will then come back to you with an estimate of how long the issue will take to fix. Once the fix is available, we will notify you and recognise your efforts on this page.

Thank You

Thanks to the following people who have helped make our products and services more secure by making a coordinated disclosure with us:

[Name/alias, Twitter handle]"

2.3 Means of Contact

The email address
securityalert@*<companydomain>*
or security@*<companydomain>*
is a de facto standard for researchers who disclose vulnerabilities to organisations. We recommend that organisations create and monitor both of these email addresses where possible.

It is important to provide a secure mechanism for communication about security issues, to avoid any risk of the communication being intercepted and the information being used maliciously.

It is recommended that organisations provide a secured web form for the initial contact message, as this does not require the reporting party to install email encryption software and the necessary encryption keys, which can be prone to error. Nevertheless, organisations should consider also publishing a public key with which emails can be encrypted for confidentiality.

2.4 Communicating with the Researcher

Security researchers may have a wide variety of backgrounds and expectations; they may be, for example, hobbyists unused to business processes, academics who desire the freedom to publish research, or professional consultants building a reputation for expertise in finding security problems. It is important, in communication with researchers, that due consideration and recognition is given to the effort that they have made into researching the particular security problem. Their motivation and expectations may well differ from yours, so it is imperative that they are given enough room to work with you and that a constructive, understanding tone is adopted at all times even if their actions may seem inappropriate in your business context.

2.5 Resolving Conflict

It is likely that at some point, there are going to be issues where both parties disagree. The Organisation for Internet Safety guidelines [OIS] included recommendations on how to resolve such conflicts in the context of an organisation's published vulnerability disclosure process. In summary:

- Leave the process only after exhausting reasonable efforts to resolve the disagreement;
- Leave the process only after providing notice to the other party;
- Resume the process once the disagreement is resolved.

2.6 Timing of Response

The text on your security contact web page should state in what time frame the security researcher can expect a response; this will typically be a few days, perhaps up to a week. It is good practice to send an automatic acknowledgement for email sent to the contact email address including the same details on the expected response time. The following response should then further clarify expectations regarding the timing of further communications and, once a problem has been confirmed, in what time frame a patch, fix or other remediation is expected to be made available.

It can be very difficult to estimate a reasonable amount of time for a security vulnerability to be fixed. It depends on many factors, including the nature of the affected component (e.g. a web service, a software product or a hardware product), the technical complexity and architectural depth of the problem, and the mechanisms available for updating the offering. It is a topic that has been debated at length amongst the security community and continues to be a source of tension.

It is important to communicate with the researcher and explain how you justify your estimated timing. If the researcher feels that you are not taking their report seriously enough, it may cause a breakdown of the process and premature public disclosure of the vulnerability. At one extreme, for a simple problem in a live web service involving individuals' personal data, a reasonable time to fix might be only a few days, but at the other extreme, fixing a complex problem with a physical product that requires new hardware to be manufactured and distributed to repair centres could take many months.

2.7 Security Advisory

The organisation should have a mechanism via which security advisories can be issued, so that users can be informed once a problem is fixed. This should be done via a secure webpage to authenticate the information. Some organisations also use security announcement mailing lists; it is good practice to digitally sign the advisory email text so that it can be authenticated.

2.8 Credit Where Credit Is Due

It is standard practice as a gesture of goodwill and recognition of security researchers' efforts to name security researchers who have cooperated in a vulnerability disclosure, although it is important to confirm their consent to this before publicly identifying them. The acknowledgement is often done on the same web page as the vulnerability disclosure policy. It is generally expected that a researcher's Twitter handle (if available) will also be included.

2.9 Money

Crediting a security researcher does not necessarily indicate that they are financially compensated and such compensation is not generally expected. Companies may wish to introduce "bug bounty" programmes or work with intermediaries who manage such programmes on behalf of companies, but this topic is out of the scope of these recommendations.

2.10 Discouraging Damaging Actions

It can be argued that, by publishing a Vulnerability Disclosure policy, organisations could be encouraging hackers in the name of security research. This is a misleading argument as, without a published policy, the organisation is turning a blind eye to research that would otherwise go on without its knowledge. Companies can fall into the trap of "shooting the messenger" when it comes to the disclosure of a vulnerability. This is why some people are suspicious of approaching a company when they discover a security issue.

A company should, however, not encourage damaging activity. Some security pages explicitly exclude certain types of research – for example Denial of Service attacks on a site or the hacking into systems in order to expose customer data. An example of this can be found in the IoT Security Foundation's own vulnerability disclosure policy: http://www.iotsecurityfoundation.org/security.

3 Internal Organisation and Processes

Successful vulnerability disclosure management must involve a nominated responsible person. It is suggested that this should be the CISO, or a Head of Security Response if one is appointed. In addition to this, it is recommended that confirmed disclosure emails sent to the disclosure email address are distributed to a list of senior staff that should be aware of disclosures that are underway. The remaining steps should continue as per the standard internal security incident handling processes of the organisation, with the added aspects of communicating with the security researcher on a regular basis to update and possibly asking for additional information or assistance. The final step is the creation of the security advisory and agreeing the "go public" date with the researcher.

There is a companion specification to ISO 29147, that is ISO/IEC 30111:2013, *Information technology -- Security techniques -- Vulnerability handling processes* [ISO2013], which goes into more detail on internal processes for handling vulnerabilities. Regardless of whether ISO 30111 is used or not, the process to be followed should be appropriately documented within the organisation.

4 References and Abbreviations

4.1 References

[ISO2013] **ISO/IEC 30111:2013, Information technology -- Security techniques -- Vulnerability handling processes**

[ISO2014] **ISO/IEC 29147:2014,** *Information technology -- Security techniques -- Vulnerability disclosure*

[OIS] **Organization for Internet Safety,** *Guidelines for Security Vulnerability Reporting and Response,* **Version 2.0, 01 Sep 2004**

4.2 Definitions and Abbreviations

Advisory	An announcement or bulletin that informs users about a vulnerability in a product or service, usually including instructions on how to remediate the vulnerability
Breach	Any incident that results in unauthorized access to data, networks, devices or services
CISO	Chief Information Security Officer
IoT	Internet of Things
IoTSF	Internet of Things Security Foundation
ISO	International Organization for Standardization
Researcher	An external discoverer of a security vulnerability (referred to in ISO 29147 as “finder”)
Vulnerability	A weakness in a system that can be exploited to compromise security
WG-4	IoTSF Working Group 4, *Framework for Vulnerability Disclosure*

IoT Security Foundation

www.iotsecurityfoundation.org