Consumer IoT Security Quick Guide:

MANAGE VULNERABILITY REPORTS

IoT Security Foundation

Implement a means to manage reports of vulnerabilities

New standards and regulation

87% of consumer IoT companies do not have a vulnerability disclosure policy.[1] However, new standards and regulations require IoT manufacturers, and some importers, to publish a vulnerability disclosure policy, to act on disclosures in a timely manner and promote coordinated vulnerability disclosure.

Standard ETSI EN 303 645[2] promotes management of vulnerabilities and requires publication of a vulnerability disclosure policy. The UK Government's Code of Practice for Consumer IoT Security[3] and Australia's Draft Code of Practice[4] set out similar requirements. The UK government is preparing legislation on securing consumer IoT, which will require IoT manufacturers to publish a vulnerability disclosure policy.[5]

Important security considerations

Even if an IoT product has no known security vulnerabilities when it is shipped, it will become vulnerable to new security threats over time. IoT manufacturers need to manage vulnerabilities because every IoT product will need to adapt to new security threats or best practices. Vulnerabilities can put user safety, personal data, devices and networks at risk. Without mechanisms for security researchers or users to report vulnerabilities, or for manufacturers to manage and resolve vulnerabilities, the security of consumer IoT will diminish over time as likelihood of attack or abuse increases. Failure by the manufacturer to respond to a reported vulnerability may result in uncontrolled public disclosure of the vulnerability or escalation, for example, to bad actors, the press, or national authority. This can cause serious harm to your business, brand image, put users at risk, and result in legal action. Additionally, because the vulnerability exists, it may already be actively exploited by bad actors.

Impact on consumer IoT manufacturers

Failure to comply with standards or regulation can result in significant reputational and financial damage to the company. Governments sometimes identify appropriate international standards, such as ETSI EN 303 645,[2] that companies can adopt to show compliance with regulation. For example, a consumer IoT manufacturer that is not able to make their vulnerability disclosure policy publicly available will not be able to claim compliance with ESTI EN 303 645[2] and may have difficulty proving compliance with national legislation. Violation of forthcoming UK regulation will likely result in sanctions, such as fines or removing products from the market.

Where to start?

Below are five key questions for managers to discuss among product development, security, and compliance teams and will help on the road to compliance with ESTI EN 303 645.[2]

- Do we have a publicly available vulnerability disclosure policy?
- Do we have an internal vulnerability management procedure?
- Where is our public contact information listed for vulnerability reporting?
- How do we continually monitor for and identify security vulnerabilities within our products?
- Are we actively following our policies and procedures?

Why it matters

- Vulnerabilities can put user safety, personal data, networks and devices at risk.
- Poorly managed vulnerability disclosure can result in reputational and financial damage.
- Failure to respond to a reported vulnerability may result in public disclosure or escalation before it is fixed , and added cost of managing duplicate reports.
- Failure to comply with regulation can result in significant penalties such as fines or removal of products from the market.

1 in 5
companies with a disclosure policy use a proxy disclosure service.[1]

Existing standards, regulation and guidance

- ETSI EN 303 645 Cyber Security for Consumer IoT (2020)[2]
- UK DCMS Code of Practice for Consumer IoT Security (2018)
- United States: California and Oregon state legislation
- Australia Draft Code of Practice: Securing the Internet of Things
- Upcoming UK Regulation for Consumer IoT Security (2021)

Dos and Don'ts: Guidance on complying with new standards and regulation

Dos

Before: **Prepare to implement a coordinated vulnerability disclosure program**

Tip: Sign up to a vulnerability management service to simplify reporting and management of vulnerabilities. IoTSF's service VulnearbleThings.com can help with vulnerability reporting, management, and coordinated disclosure.

Have a publicly available coordinated vulnerability disclosure policy[6] that is clear and transparent. The policy should set expectations of parties and include information like:

- Directions and expectations for submitting a report posted on a webpage such as IoTcompany.com/security and as a published security.txt file.
- A public point of contact such as an email (e.g. security@IoTcompany.com), webform, or vulnerability management service used to submit a report.
- Information on timelines for responding to the reporter including acknowledging receipt of the report, and regular status updates until the vulnerability is resolved. Recommendations are included in the "During" section.
- Where to find published security advisories. This might be a webpage on the company's own website or on a service like VulnerableThings.com.
- Clear expectations for security researchers such as not accessing more personal data than is necessary to demonstrate a vulnerability and not DDoSing a service.
- Legal obligations for those involved.

Have an internal vulnerability management plan so that you are prepared to respond to a report and follow coordinated vulnerability disclosure best practices. An internal policy should include information like:

- Standard process and documented procedures to follow to address a vulnerability from report or discovery to disclosure.
- Timelines for vulnerability resolution and disclosure.
- Onboarding and training of relevant parties across the organization.
- A single point of contact to manage external communications who is familiar with security terminology and the vulnerability disclosure process.

Don'ts

- Do not ignore vulnerability reports. Instead, prepare by implementing a coordinated vulnerability disclosure policy and management plan.
- Do not publicly disclose the vulnerability before it has been resolved.
- Do not interact with the reporter in a hostile or negative manner. Reporting a vulnerability provides the company an opportunity to resolve the issue before it is published or, worse, exploited. It also means the product is worth researching and improving.
- Do not forget about local data protection legislation. If the vulnerability has already compromised data or personal information, you must comply with local legislation. For example, you may need to submit a report to the national Data Protection Authority.

During: **Work together and address the vulnerability**

- Acknowledge receipt of the vulnerability as soon as possible, but within 7 days.
- Work with the reporter to understand and resolve the vulnerability.
- Aim to resolve any software vulnerabilities within 90 days.
- Take appropriate measures to mitigate risks posed by the vulnerability, including temporary measures.
- Use secure communication methods, like PGP encrypted emails, where possible when communicating about the vulnerability with others, such as coordinating with the vulnerability reporter.
- Engage professionally with the vulnerability reporter and adopt a positive mindset. Reporting a vulnerability helps your company and your product be more secure.

After: **Coordinated vulnerability disclosure**

- Work with the reporter to publicly disclose the vulnerability and fix at the same time.
- Acknowledge the reporter's efforts by crediting them, for example in the coordinated vulnerability disclosure and in communications about the vulnerability.

Things to think about going forward

In addition to the basic dos and don'ts, here are a few more areas that need to be considered when managing vulnerability disclosures.

- Identify the external dependencies and key contacts in software and hardware supply chains.
- Discuss coordinated vulnerability disclosure with your supply chain, including what processes are in place, the role of each party, and communication methods.
- Consider establishing a "bug bounty" scheme which rewards reporters for their efforts.
- Consider sharing intelligence after disclosure, for example with public repositories (e.g. Mitre's CVE[7]) or industry bodies (e.g. IoTSF[8] or GSMA[9]).
- Review your vulnerability report management process. What lessons have been learned, for example, about your product, development process or vulnerability preparedness?
- Work with the security research community to better understand how consumer IoT is targeted and how better to address product security issues. Examples include attending security research and hacking conferences.

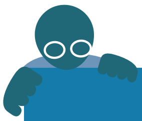
Where to go for more information?

From IoT Security Foundation

- IoTSF's Vulnerable Things service[10]
- IoTSF Vulnerability Disclosure Best Practice Guidelines[11]
- IoTSF consumer IoT security resources[12]
- IoTSF's live training webinars

From other bodies

- UK NCSC's forthcoming vulnerability disclosure toolkit (2020)
- hackerone's Vulnerability Disclosure Policy Basics[13]
- OWASP vulnerability disclosure cheat sheet[14]
- IETF's security.txt (draft standard)[15]
- ISO/IEC 29417:2018[16]
- ISO/IEC 30111:2019[17]
- NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers[18]



Who should see this:

It is critical that people with different roles and responsibilities are aware of coordinated vulnerability disclosure standards and regulation, and how they impact the organization. Examples of who should see this include:

Compliance Officer: The compliance officer is responsible for how the organization respects the principals in this guide, standards, regulations and/or code of practice.

Board of Directors: Board buy-in is essential in order to allocate resources for vulnerability management and response as well as preparation (e.g. public polices, internal procedure).

Product Manager: Buy in from the product manager is also critical. The product manager needs to coordinate the different parties working to resolve and fix a vulnerability and feed into coordinated disclosure when appropriate.

Product Development Manager: The product development manager is crucial to ensuring the reported vulnerability goes through the appropriate management process, particularly validating and fixing vulnerabilities in the product.

Product Security Team: The product security team oversees implementation of security in the product, including changes in response to vulnerabilities or preparing security updates.

Supply Chain Manager: A vulnerability may need to be responsibly disclosed within a supply chain – for example if the vulnerability impacts integrated equipment, or if it originates with a supplier's product. The supply chain manager can help identify who should be notified and manage relations.

Head of Public Relations: During coordinated vulnerability disclosure, public relations may assist with publishing information and guiding the discussions related to a reported vulnerability.

What are the Consumer IoT Security Quick Guides?

The “Consumer IoT Security Quick Guides” identify best practices to help organizations around the world understand and comply with new international standards, regulations and national guidance on consumer IoT security. These Quick Guides demystify high level language, point to additional information, and provide different ways of thinking about or alternative approaches to consumer IoT security.

The Quick Guides build upon the ETSI EN 303 645[2] specification on consumer IoT cybersecurity. It is the first international standard of its kind. Based upon it, governments are publishing Codes of Practice[19] and are preparing legislation[20] that impact companies developing, manufacturing or providing consumer IoT products. The Quick Guide series focuses on the top 3 issues identified in standards and guidance: passwords, vulnerability disclosure, and software updates.[3]

Footnotes

[1] https://www.iotsecurityfoundation.org/wp-content/uploads/2020/03/IoTSF-2020-Progress-Report-Consumer-IoT-and-Vulnerability-Disclosurev2.pdf
[2] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
[4] https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
[5] The regulatory proposals are currently subject to a public call for views and might change as a result.
[6] See www.vulnerablethings.com public resources for samples and more information.
[7] https://cve.mitre.org/
[8] https://www.iotsecurityfoundation.org/
[9] https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/
[10] https://www.vulnerablethings.com
[11] https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf
[12] http://www.iotsecurityfoundation.org/consumer-iot
[13] https://www.hackerone.com/blog/Vulnerability-Disclosure-Policy-Basics-5-Critical-Components
[14] https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html
[15] https://datatracker.ietf.org/doc/draft-foudil-securitytxt/
[16] https://www.iso.org/standard/72311.html
[17] https://www.iso.org/standard/69725.html
[18] https://csrc.nist.gov/publications/detail/nistir/8259/final
[19] For example, the UK and Australia
[20] For example, US states Oregon and California, and the UK.

Copyright, Trademarks and Licensing

Acknowledgements

This guidance was commissioned by the Department for Digital, Culture, Media & Sport (DCMS) and delivered by the IoT Security foundation in partnership with Oxford Information Labs.

We wish to acknowledge significant contributions from IoTSF members to this version of the document

Stacie Hoffmann and Patrick Taylor, Oxford Information Labs
David Rogers, Copper Horse

Peer reviewers:
Roger Shepherd, Chipless
Trevor Hall, DisplayLink
Richard Marshall, Xitex Ltd
Claire Milne, independent consultant

Plus others – you know who you are!

IoT Security Foundation

Department for Digital, Culture, Media & Sport

In partnership with
OXFORD INFORMATION LABS