MANAGE VULNERABILITY REPORTS

Emily Taylor, Oxford Information Labs

David Rogers, Copper Horse

IoT Security Foundation

OXFORD INFORMATION LABS

Course Aims

Participation in this course should result in an understanding:

- Of new guidance, EN 303 645, and upcoming regulation
- Of coordinated vulnerability disclosure (CVD)
- Of how to be prepared for vulnerability disclosure
- Of how to operate a coordinated vulnerability disclosure scheme

Learning outcomes

By the end of the course, you should understand:

- The importance of coordinated vulnerability disclosure
- Who the key players are and how they interact
- The process of coordinated vulnerability disclosure
- What is and why to adopt a coordinated vulnerability disclosure scheme

Security and Technical Education Programme (STEP)

- IoT Security Foundation Quick Guides & training webinars
  - No universal default passwords
  - Managing coordinated vulnerability disclosure
  - Security software updates
- Industry and private sector-led
- Worked closely with UK government
- Technical and regulatory experts

IoT Security Foundation

OXFORD INFORMATION LABS

Who is this course aimed at?

SMEs, start-ups, innovators and researchers

Engage people across the organization…

- Compliance officer
- Board of Directors
- Product Manager
- Product Development Manager
- Product Security Team
- Supply Chain Manager
- Head of Public Relations

IoT Security Foundation

OXFORD INFORMATION LABS

Meet the presenters

IoT Security Foundation

OXFORD INFORMATION LABS

Standards and regulation

What's the problem with vulnerability disclosure?

87%

of consumer IoT companies don't have a vulnerability disclosure policy

IoT Security Foundation

OXFORD INFORMATION LABS

Standards and regulatory change

Standards

- ETSI EN 303 645 Consumer IoT cybersecurity
- Subject-specific standards
  - ISO/IEC 29147_2018 – Vulnerability Disclosure
  - IETF security.txt – File Format to Aid security Vulnerability Disclosure

Regulation

- US: California Senate Bill #327, Oregon House Bill #2395
- UK: Proposal for regulating consumer smart product cyber security (summer 2020 – consultation on draft legislation)

What guidance is available?

- Subject-specific guidance
  - IoTSF Quick Guides
  - IoTSF Best Practice Guides
  - UK NCSC

Codes of Practice

- UK: Code of Practice for Consumer IoT Security
- Australia: code of practice
- Singapore: cybersecurity labelling scheme

ETSI: Cybersecurity for Consumer Internet of Things Baseline Requirements

ETSI EN 303 645

- First international standard of its kind
- ”Brings together widely considered good practice…baseline provisions.”
- “As consumer IoT products become increasingly secure, it is envisioned that future revisions of the present document will **mandate** provisions that are currently recommendations”

Legislation is making these provisions mandatory

IoT Security Foundation

OXFORD INFORMATION LABS

ETSI standard – in brief

Top 3 Covered in this webinar series:

- No universal default passwords
- **Implement a means to manage reports of vulnerabilities**
- Keep software updated

Others:

- Securely store sensitive security parameters
- Communicate securely
- Minimize exposed attack surfaces
- …And more!

IoT Security Foundation

OXFORD INFORMATION LABS

UK proposed regulation overview

Aim: Establish a cybersecurity baseline for consumer IoT products

What does it say *now*?

- Applies to network-connectable consumer IoT products
  - “has one or more network interface that can receive and/or transmit digital data”
  - Consumer market, but could be used by businesses
- Sets out obligations for IoT producers and duty of care for distributors
- Products that do not comply should not be ”supplied or made available to consumers” on the UK market

Failure to comply? Fines or removing products from the market

IoT Security Foundation

OXFORD INFORMATION LABS

Requires publication of a vulnerability disclosure policy

…and implementation of a means to manage vulnerabilities.

Vulnerability Disclosure Policy…

- Publicly available, clear, and transparent
- Reporting allowed in an ‘accessible’ way
- Include contact info and timelines

Why?

- Vulnerabilities put users, data, devices and networks at risk
- Without a reporting mechanism issues cannot be flagged (or fixed)
- Failure to respond could result in unfavorable disclosures or damage to your brand

IoT Security Foundation

OXFORD INFORMATION LABS

How can this webinar and Quick Guide help?

- Understanding coordinated vulnerability disclosure
- Guidance on preparing a public vulnerability disclosure policy
- Best practices for responding to and managing a disclosure

Look out for other resources in this series

Free! Webinars on Vulnerability Disclosure and Software Updates

Free! Quick guides to complement the webinar topics https://www.iotsecurityfoundation.org/consumer-iot/

VulnerableThings.com …a vulnerability disclosure platform for consumer IoT supply chain.

Recommendations and Standards

- ISO/IEC: 30111 Information technology — Security techniques — Vulnerability handling processes
- ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure
- IoTSF: Vulnerability Disclosure Best Practice Guidelines, Rel. 1.1
- ETSI EN 303.645 Cyber Security for Consumer Internet of Things: Baseline Requirements
- IETF draft informational RFC ‘A File Format to Aid in Security Vulnerability Disclosure’

VULNERABLE THINGS

About FAQs Report Join Sign in

Report Vulnerability

Report a vulnerability with a 'thing' or device. Report anonymously or get public acknowledgement.

Join

Join as a member. Easily comply with disclosure requirements. Manage disclosures. Get help.

Consumer Internet of Things Vulnerability Disclosure Platform

Free to report vulnerabilities. Join to manage reports and publish disclosures.

Report Vulnerabilities | Manage reports | Publish coordinated vulnerability disclosures | Access resources

Read more >

IoTSF Website: Manage Vulnerability Reports Quick

Twitter: UK Minister Minister for Digital Infrastructure

IoT Security Foundation

OXFORD INFORMATION LABS

MANAGE VULNERABILITY REPORTS

David Rogers, Copper Horse

IoT Security Foundation

OXFORD INFORMATION LABS

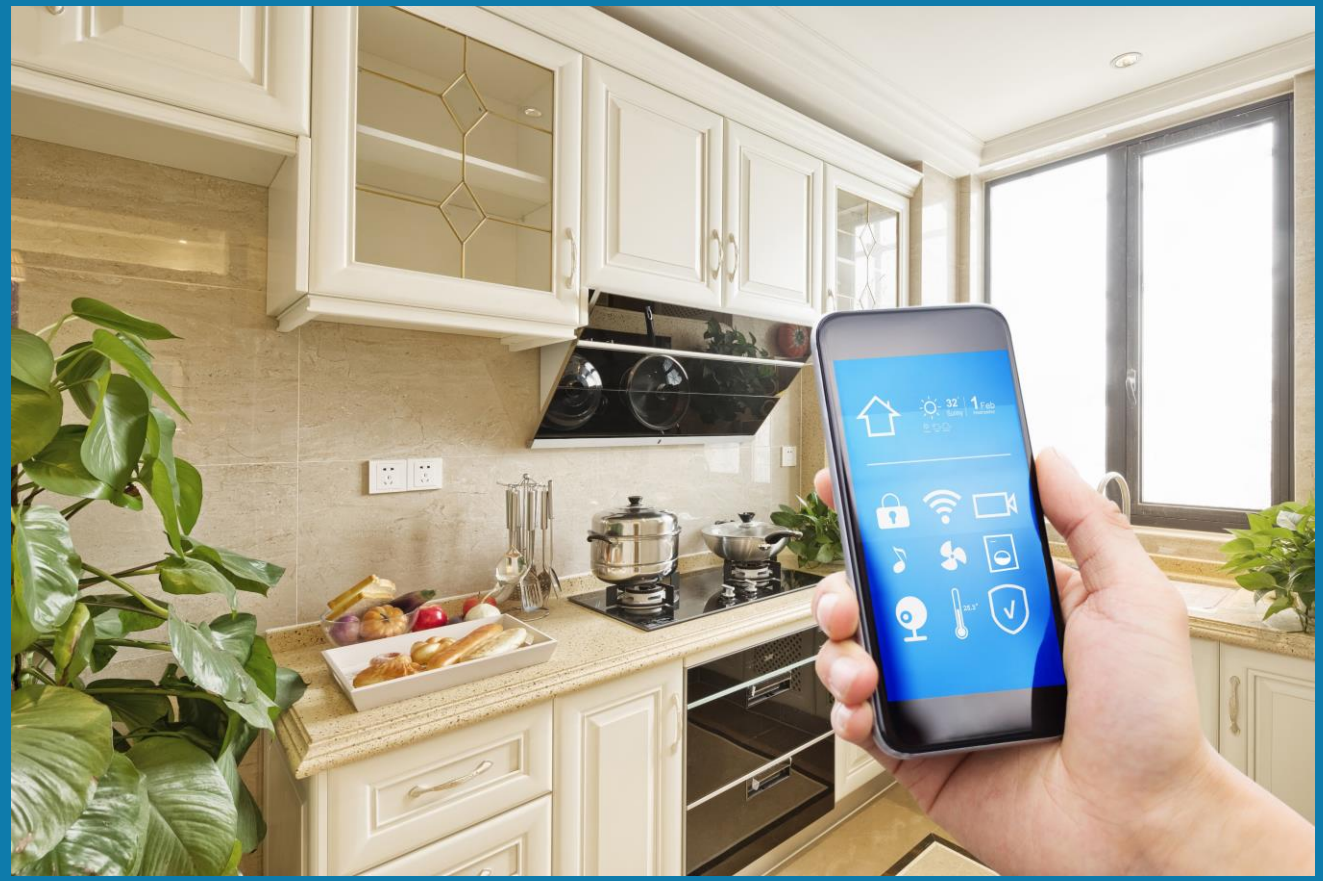
What is Vulnerability Disclosure?

- A set of rules for how companies and security researchers can interact in a way which penalises neither.
- An important component in overall cyber security and keeping users safe

IoT Security Foundation

OXFORD INFORMATION LABS

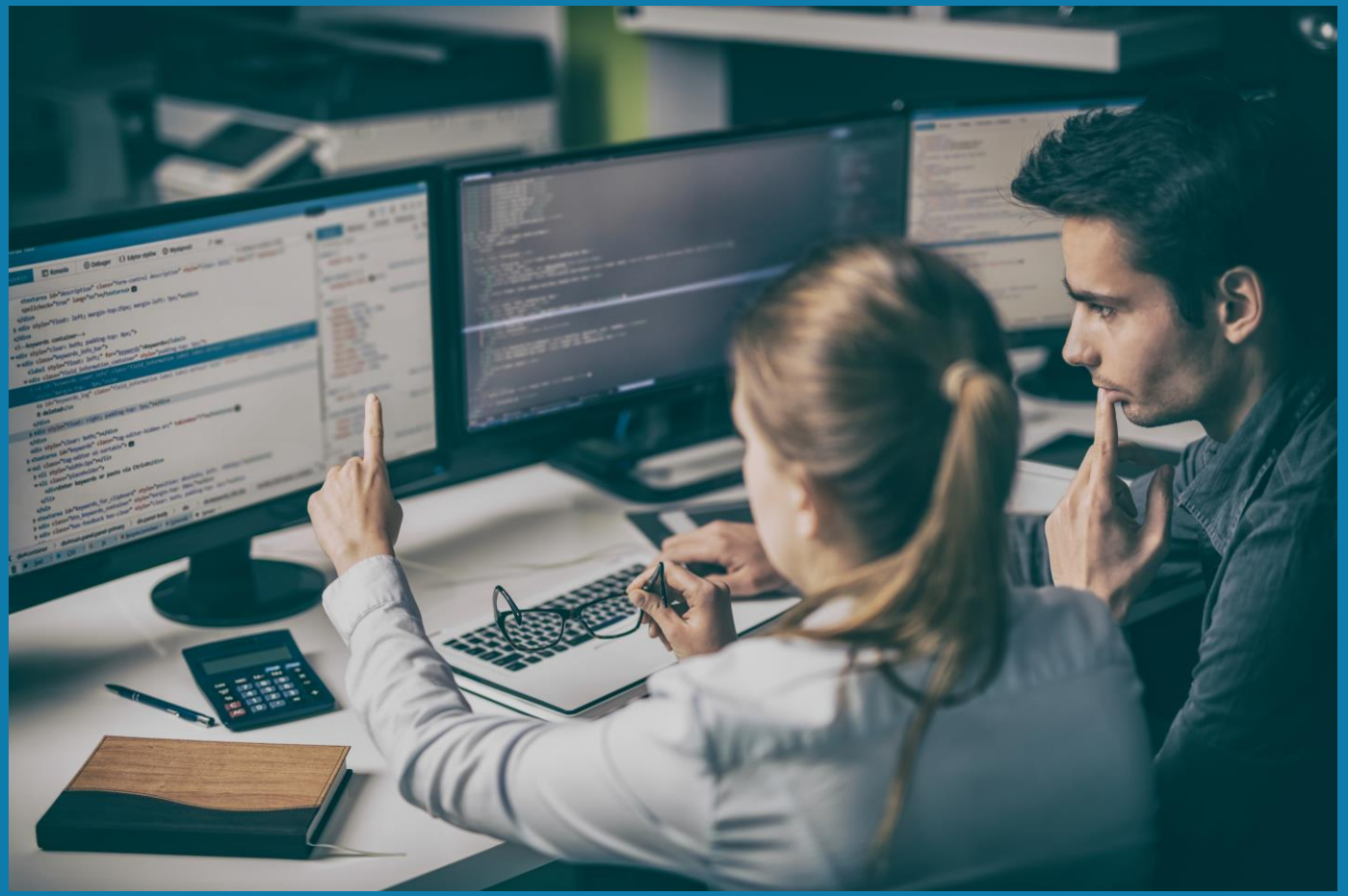
What do we mean by vulnerabilities?



IoT Security Foundation

OXFORD INFORMATION LABS

Who are security researchers?

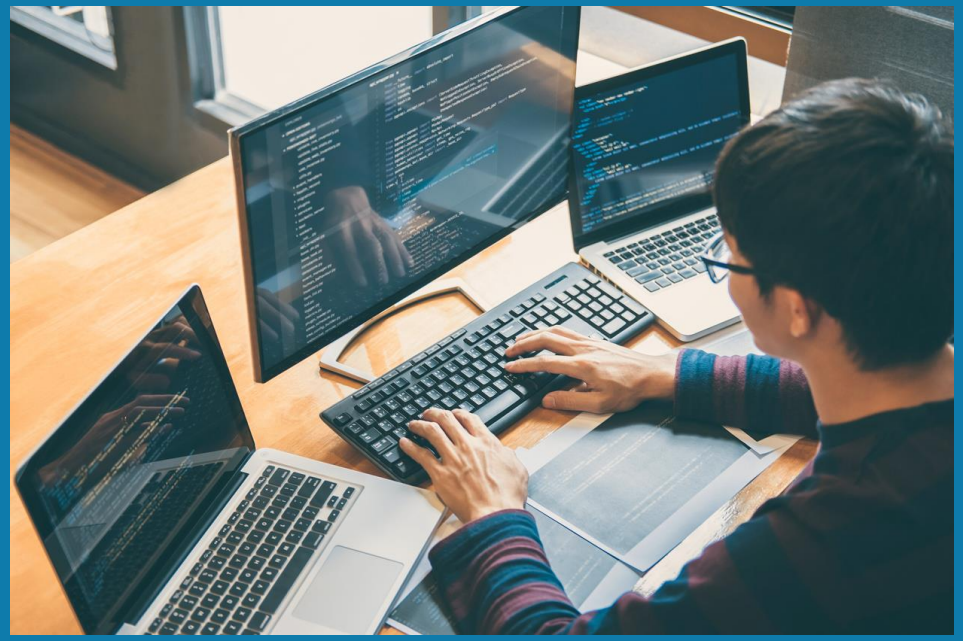


IoT Security Foundation

OXFORD INFORMATION LABS

Why should I talk to a security researcher?

- Security incidents are made worse if your company doesn't even know about the issue!
- Security researchers / reporters are trying to help you.



IoT Security Foundation

OXFORD INFORMATION LABS

History and types of disclosure

- Non-Disclosure
- Limited Disclosure
- Full-Disclosure
- RFPolicy
- **Coordinated Vulnerability Disclosure**

- “Responsible” Disclosure is subjective terminology

Where are we now?

DZone A DEVADA MEDIA PROPERTY IoT Zone Over a million developers have join

REFCARDZ RESEARCH WEBINARS | Agile AI Big Data Cloud Database DevOps Integration IoT Java Microservices Open Source

The Disastrous State of IoT Vulnerability Reporting

Less than 10% of consumer IoT brands have a reporting process.

by Mike Gates STAFF MVB · Dec. 21, 18 · IoT Zone · News

Like (2) Comment (0) Save Tweet 9,051 Views

Join the DZone community and get the full member experience. JOIN FOR FREE

It's no secret that IoT security is one of the biggest oxymorons in tech.

One would think that after two years of some of the worst security breaches on the planet

IoT Security Foundation

OXFORD INFORMATION LABS

Process Establishment and Readiness

- Basic precursors
- Internal homework!

Means of contact

- Email address, usually:
  - security@..
- Also – a duty on the company involved to ensure that administrators of addresses like postmaster@... and customer service departments know how to re-direct misdirected disclosures.
- Some organisations recommend a secure web-form to contact
- Companies sometimes publish encryption keys for secure contact

Website and Vulnerability Disclosure Policy (VDP)

- Webpage: https://[companywebdomain]/security

"[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@<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 us to continue to our millions of users out there by making a vulnerability disclosure to us:

David Rogers, @drogersuk
Xxxx, @xxxx

IoT Security Foundation

OXFORD INFORMATION LABS

‘Unacceptable’ security research?

How does a security researcher interpret this?

[Organisation] does not permit the following types of security research:

Causing or attempting Denial of Service.
The attempted or actual destruction or corruption of data.
The attempted or actual access to personal or private data.
The interception of communications on a network that the public has access to.

- Some companies choose to outline this
- e.g. research that would disclose customer data
- Companies should not encourage damaging behaviour

IoT Security Foundation

OXFORD INFORMATION LABS

security.txt

- BBC example: https://www.bbc.co.uk/.well-known/security.txt

```
# British Broadcasting Corporation - reporting security vulnerabilities to the BBC

# Please report any security vulnerabilities to us via the contact method(s) below, only after reading our disclosure policy.
# Please do not include any sensitive information in your initial message, we'll provide a secure communication method in our reply to you.
Contact: mailto:security@bbc.co.uk

# Our disclosure policy. By submitting a potential security incident to us, you are implicitly accepting these terms - please read this before submitting:
Policy: https://www.bbc.com/backstage/security-disclosure-policy/

# We're continually recruiting, please visit the link below and search for "information security" if you're interested in a career with the BBC in infosec
Hiring: https://careerssearch.bbc.co.uk/jobs/search

# Please see https://securitytxt.org/ for details of the specification of this file
```

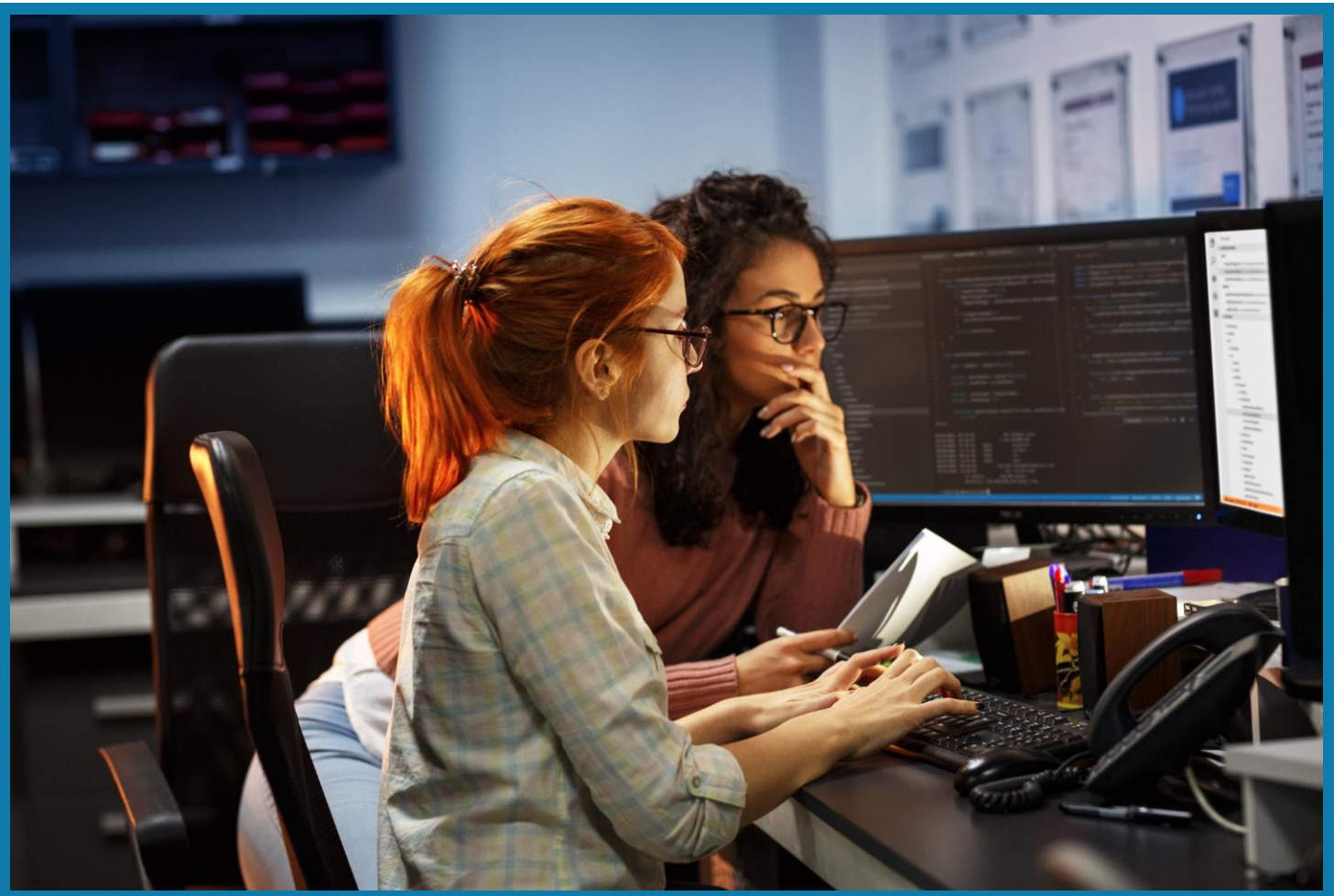
Operating a CVD scheme - walkthrough

- The disclosure
- Time – responding and total timeline

Working with the researcher

- Consider that the researcher's circumstances are very different to yours. What motivates them?
- Avoid conflict.

Addressing the vulnerability



Going public

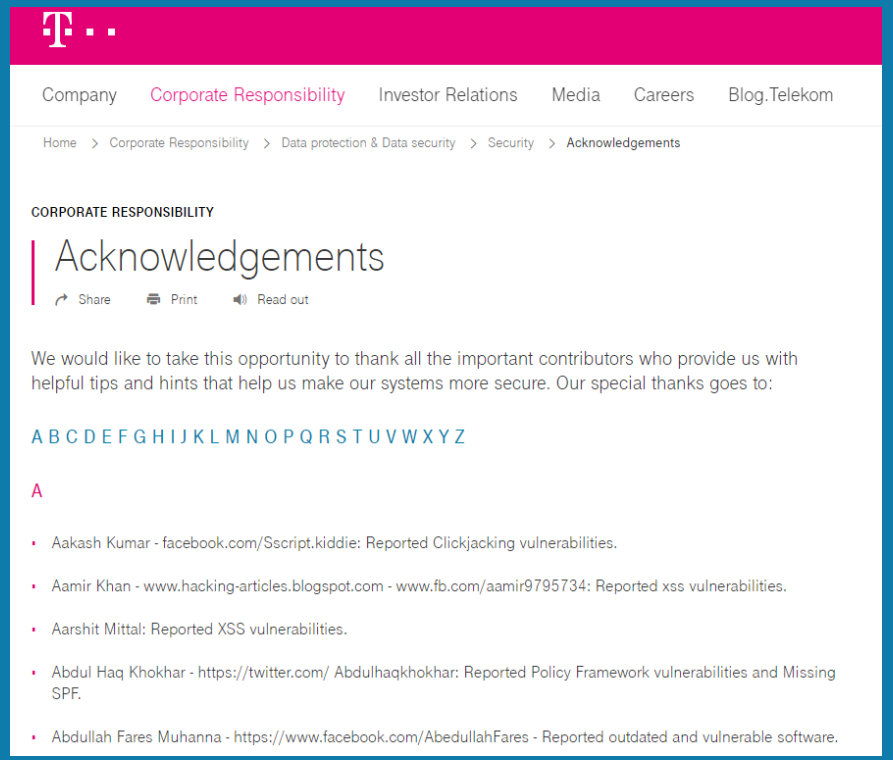
- Security Advisory
- Coordinated!

IoT Security Foundation

OXFORD INFORMATION LABS

Crediting the researcher

- Acknowledge the security researcher for their efforts:
  - List their name and twitter handle on the security page
  - Thanks in public facing PR



T · ·

Company Corporate Responsibility Investor Relations Media Careers Blog.Telekom

Home > Corporate Responsibility > Data protection & Data security > Security > Acknowledgements

CORPORATE RESPONSIBILITY

Acknowledgements

Share Print Read out

We would like to take this opportunity to thank all the important contributors who provide us with helpful tips and hints that help us make our systems more secure. Our special thanks goes to:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

- Aakash Kumar - facebook.com/Sscript.kiddie: Reported Clickjacking vulnerabilities.
- Aamir Khan - www.hacking-articles.blogspot.com - www.fb.com/aamir9795734: Reported xss vulnerabilities.
- Aarshit Mittal: Reported XSS vulnerabilities.
- Abdul Haq Khokhar - https://twitter.com/ Abdulhaqkhokhar: Reported Policy Framework vulnerabilities and Missing SPF.
- Abdullah Fares Muhanna - https://www.facebook.com/AbedullahFares - Reported outdated and vulnerable software.

https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/security/details/acknowledgements-358300

IoT Security Foundation

OXFORD INFORMATION LABS

Example disclosures

IoT Security Foundation

OXFORD INFORMATION LABS

Conclusions and Further Resources

CVD schemes in the wild

- Examples
- Proxy Disclosure

Recommendations and Standards

- ISO/IEC: 30111 Information technology — Security techniques — Vulnerability handling processes
- ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure
- IoTSF: Vulnerability Disclosure Best Practice Guidelines, Rel. 1.1
- ETSI EN 303.645 Cyber Security for Consumer Internet of Things: Baseline Requirements
- IETF draft informational RFC ‘A File Format to Aid in Security Vulnerability Disclosure’