Responsible, Coordinated, Frustriert? Vulnerability Reporting in der Praxis

Julian Suleder, ERNW Enno Rey Netzwerke GmbH

OWASP Stammtisch Heilbronn-Franken, 24.07.2025

ERNW
providing security.

whoami - Julian Suleder

- Senior Security Analyst & Researcher @
  ERNW Enno Rey Netzwerke GmbH in Heidelberg
  - Teamleiter Penetration Testing
  - Organisation von Research
  - Hauptverantwortlicher für Vulnerability Disclosures
  - Besonderes Interesse: Sicherheit von Medizinprodukten
- Studium Medizinische Informatik @ HD/HN

Responsible vs. Coordinated Disclosure

- Responsible Disclosure fokussiert das Verhalten des Meldenden
- Immer häufiger: Coordinated Vulnerability Disclosure (CVD)
  → Partnerschaftlichkeit: Schwerpunkt auf Zusammenarbeit
  → keine moralisierende Rollenbeschreibung der Researcher
  → Ziel: sicherer, fairer Ablauf, Bewusstsein für Verantwortung

BREAKING

April 25, 2025 by Malte Heinzelmann

Vulnerability Disclosure: Restricted Shell Breakout (CVE-2025-1950) and Privilege Escalation (CVE-2025-1951) in IBM Power Hardware Management Console (HMC)

BREAKING

November 27, 2024 by Marius Walter

Vulnerability Disclosure: Command Injection in Kemp LoadMaster Load Balancer (CVE-2024-7591)

BREAKING

May 22, 2024 by Daniel Schlecht

Security Advisory: Achieving PHP Code Execution in ILIAS eLearning LMS before v7.30/v8.11/v9.1

BREAKING

June 17, 2025 by Nils Emmerich

Disclosure: Multiple Vulnerabilities in X.Org X server prior to 21.1.17 and Xwayland prior to 24.1.7

BREAKING

May 5, 2025 by Florian Port

Full Disclosure: Multiple Rundeck Job Command Injections

BREAKING

November 22, 2024 by Nils Emmerich

Vulnerability Disclosure: Authentication Bypass in Vaultwarden versions < 1.32.5 - CVE-2024-55225

BREAKING February 22, 2021 by Julian Suleder

ManiMed: Hamilton Medical AG – HAMILTON-T1 Ventilator Vulnerabilities

BREAKING January 25, 2021 by Julian Suleder

ManiMed: Philips Medizin Systeme Böblingen GmbH – IntelliVue System Vulnerabilities

BREAKING July 29, 2021 by Julian Suleder

ManiMed: Ypsomed AG – mylife YpsoPump System Vulnerabilities

BREAKING April 23, 2020 by Julian Suleder

Medical Device Security: HL7v2 Injections in Patient Monitors

BREAKING February 1, 2021 by Julian Suleder

ManiMed: Innokas Yhtymä Oy – VC150 Patient Monitor Vulnerabilities

BREAKING September 11, 2020 by Julian Suleder

ERNW White Paper 69 – Safety Impact of Vulnerabilities in Insulin Pumps

BREAKING February 15, 2021 by Julian Suleder

ManiMed: B. Braun Melsungen AG – Space System Vulnerabilities

Zero-Day: Bluetooth-Lücke macht Millionen Kopfhörer zu Abhörstationen

Der in beliebten Modellen großer Hersteller verbaute Bluetooth-Chipsatz ist angreifbar. Hacker konnten so Anrufe starten und Geräte abhören.

https://www.heise.de/news/Zero-Day-Bluetooth-Luecke-macht-Millionen-Kopfhoerer-zu-Abhoerstationen-10457857.html

147

Die Verbindung zwischen drahtlosen Kopfhörern und Smartphones ist das Ziel des neuen Bluetooth Angriffs. Im Symbolbild hängen beide jedoch an einem Kabel. (Bild: Shutterstock/carballo)

26.06.2025, 12:15 Uhr Lesezeit: 8 Min. | Security

Z+ Sicherheitslücke bei Sony, Bose & Co.

Millionen Kopfhörer sind abhörbar

e Schwachstelle liegt bei einem unbekannten Chiphersteller. ngreifer können mithören und Smartphones übernehmen. Betroffen sind auch Modelle von Sony, Bose und JBL.

Von Eva Wolfangel

Quelle: https://www.zeit.de/digital/datenschutz/2025-06/sicherheitsluecke-software-bluetooth-kopfhoerer-spionage-daten?freebie=9ae5139c

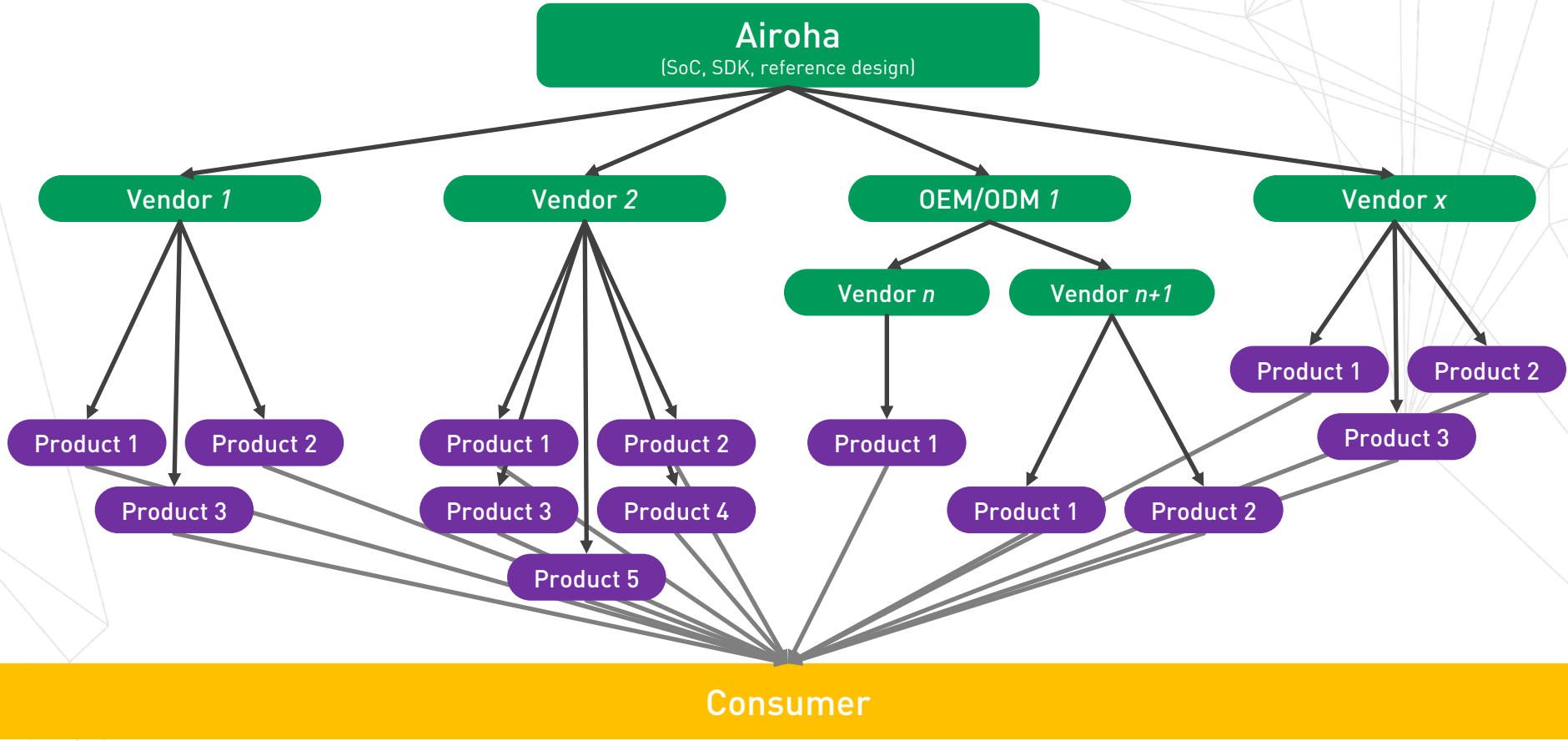
Security Advisory: Airoha-based Bluetooth Headphones and Earbuds

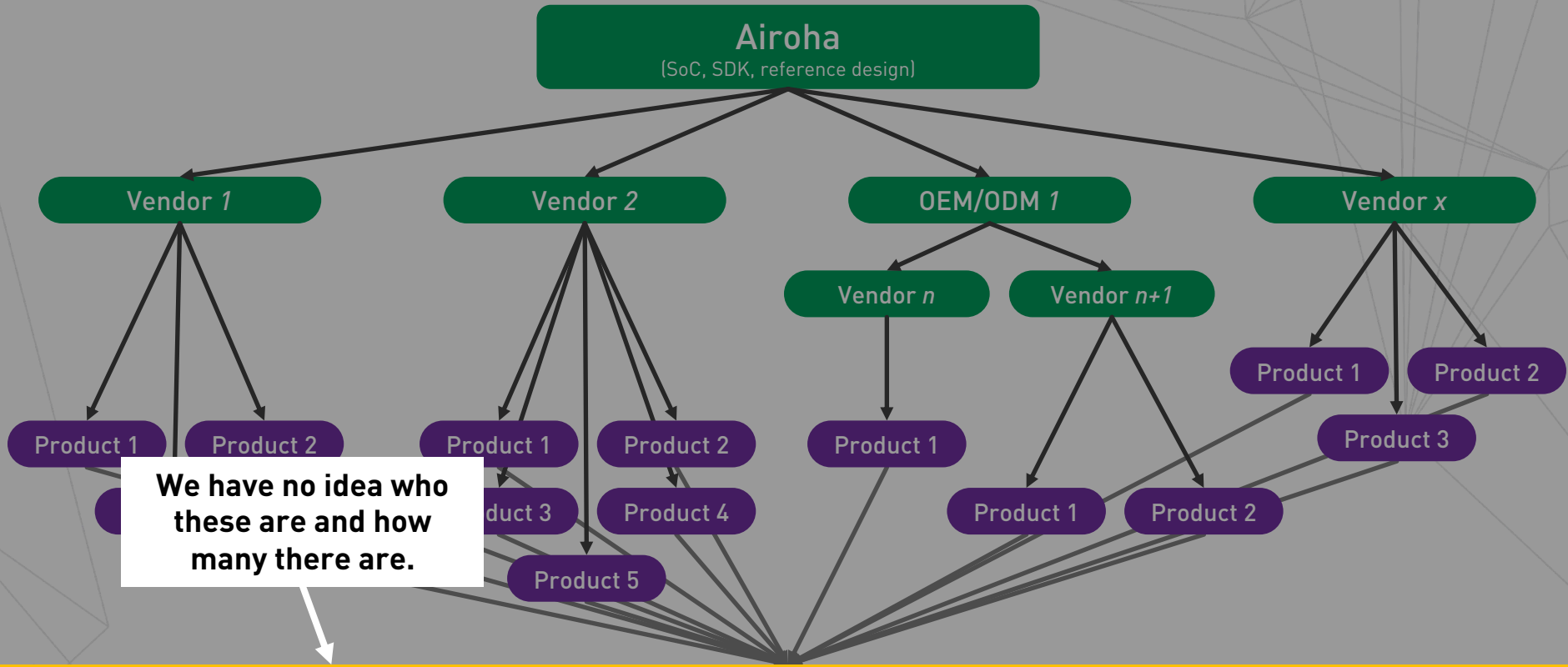
Dennis Heinze, Frieder Steinmetz

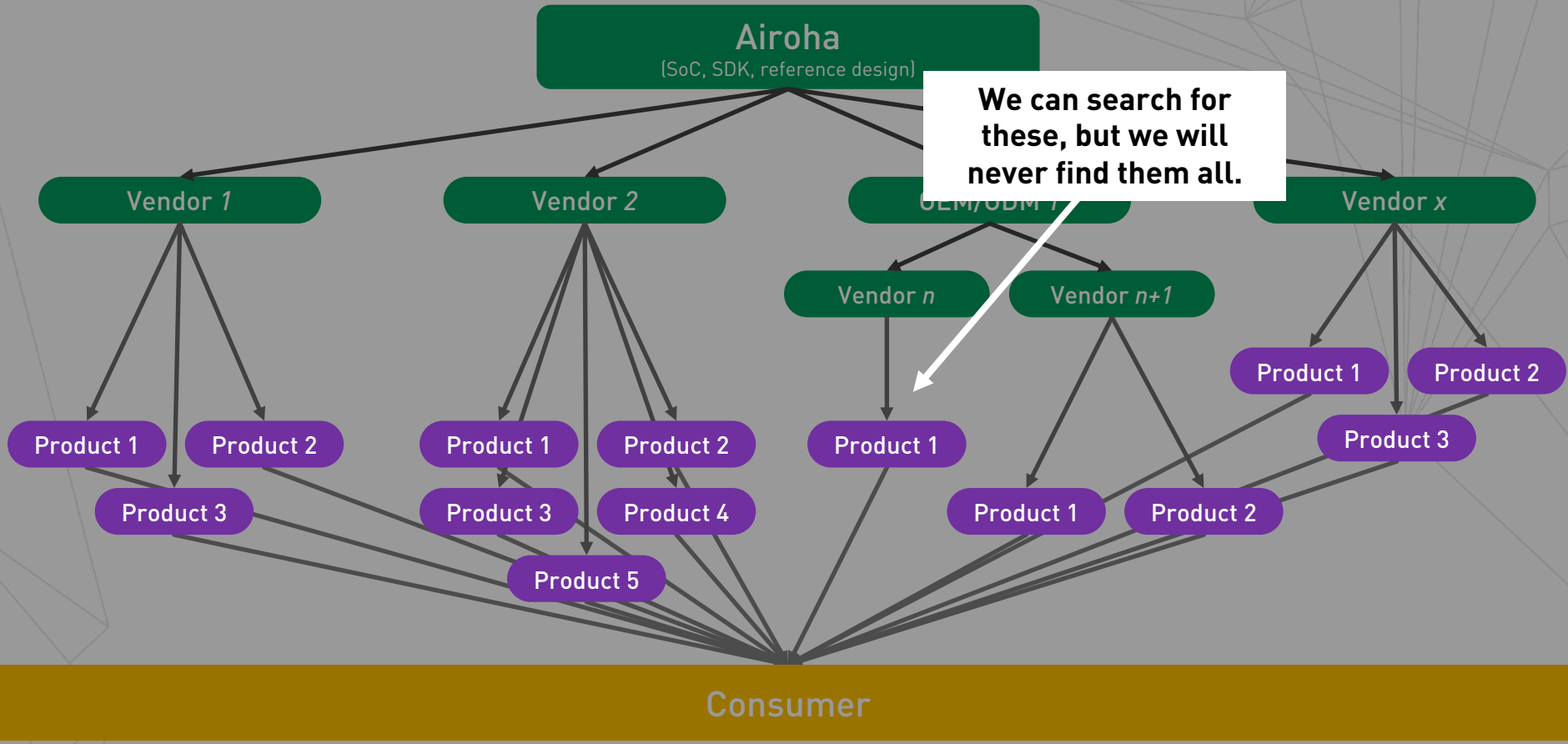
Important note: Some media coverage on this topic falsely or inaccurately depicts the attack conditions. To be clear: Any vulnerable device can be compromised if the attacker is in Bluetooth range. That is the only precondition.

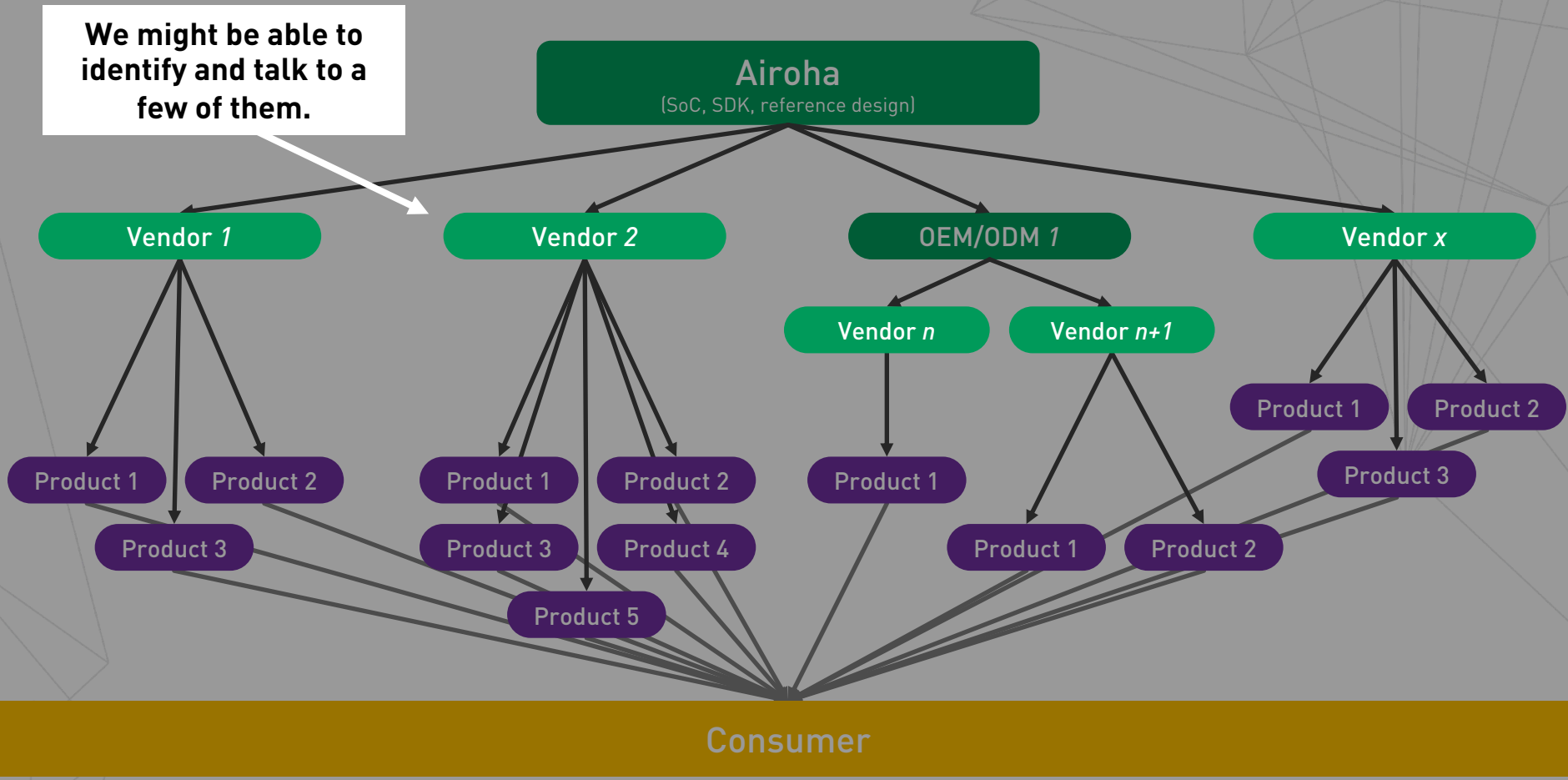
During our research on Bluetooth headphones and earbuds, we identified several vulnerabilities in devices that incorporate Airoha Systems on a Chip (SoCs). In this blog post, we briefly want to describe the vulnerabilities, point out their impact and provide some context to currently running patch delivery processes as described at this year's TROOPERS Conference.

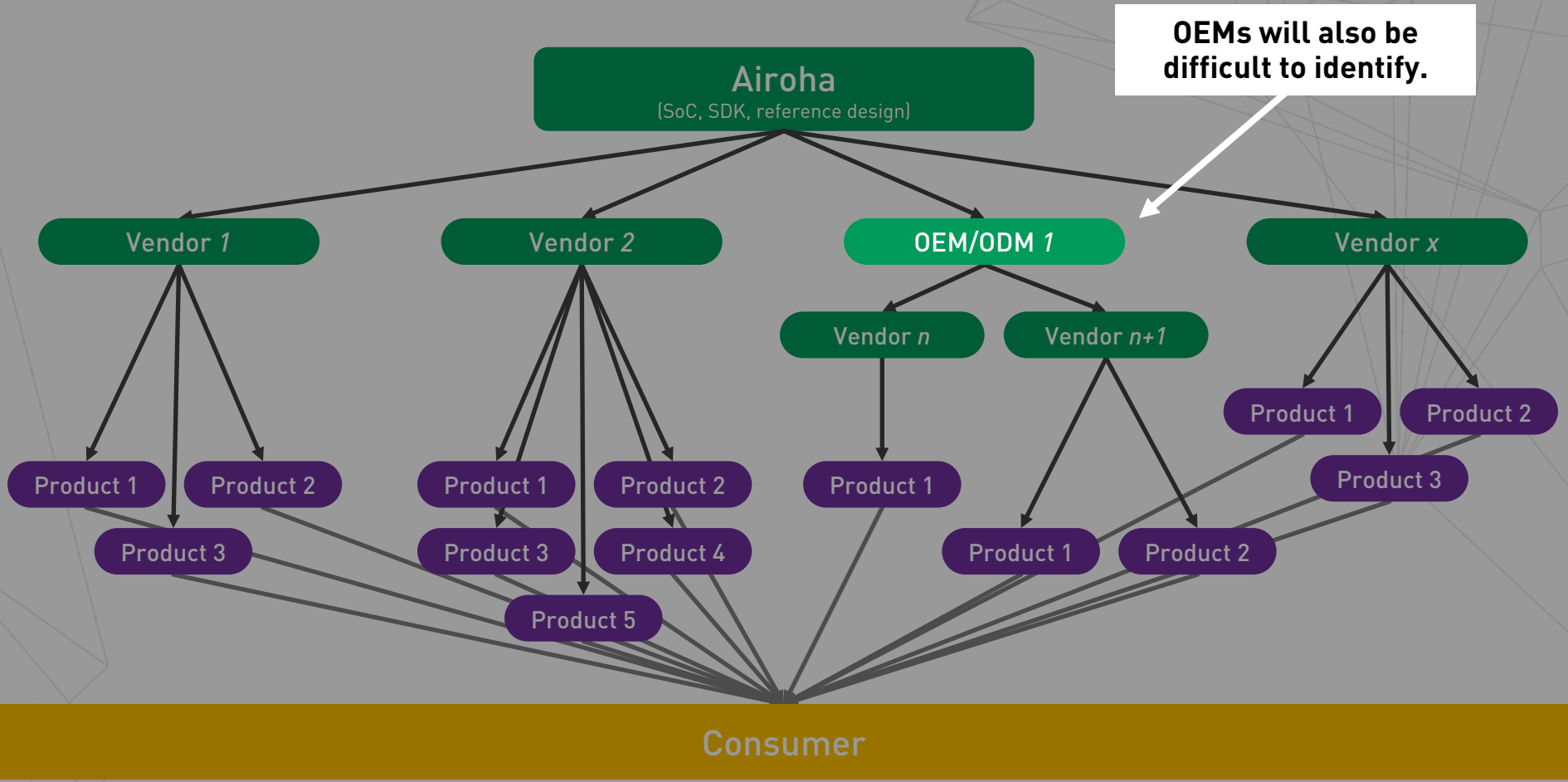
25.06.2025: https://insinuator.net/2025/06/airoha-bluetooth-security-vulnerabilities/


Airoha
(SoC, SDK, reference design)
Vendor 1
Vendor 2
OEM/ODM 1
Vendor x
Vendor n
Vendor n+1
Product 1
Product 2
Product 3
Product 4
Product 5
Consumer

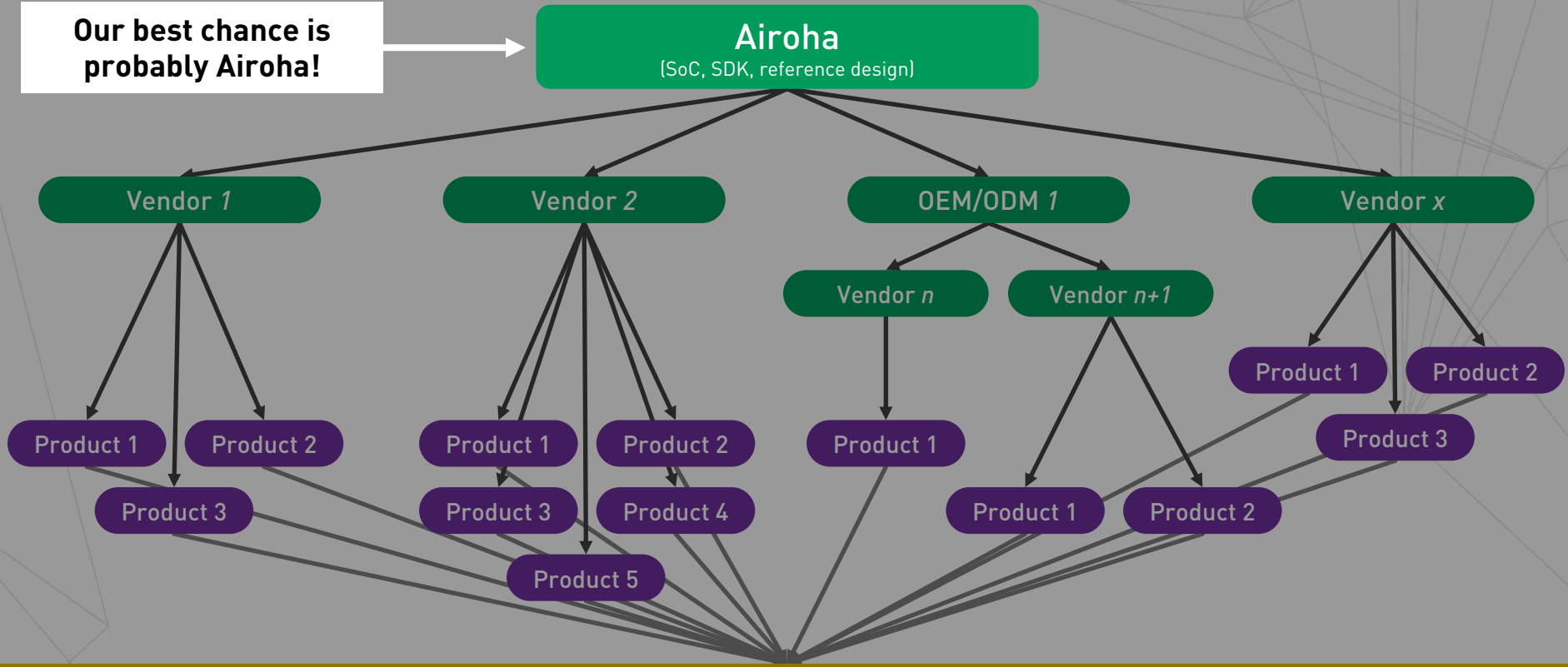

Airoha
(SoC, SDK, reference design)
Vendor 1
Vendor 2
OEM/ODM 1
Vendor x
Vendor n
Vendor n+1
Product 1
Product 2
Product 1
Product 2
Product 1
Product 1
Product 2
Product 3
duct 3
Product 4
Product 1
Product 2
Product 5
We have no idea who these are and how many there are.
Consumer

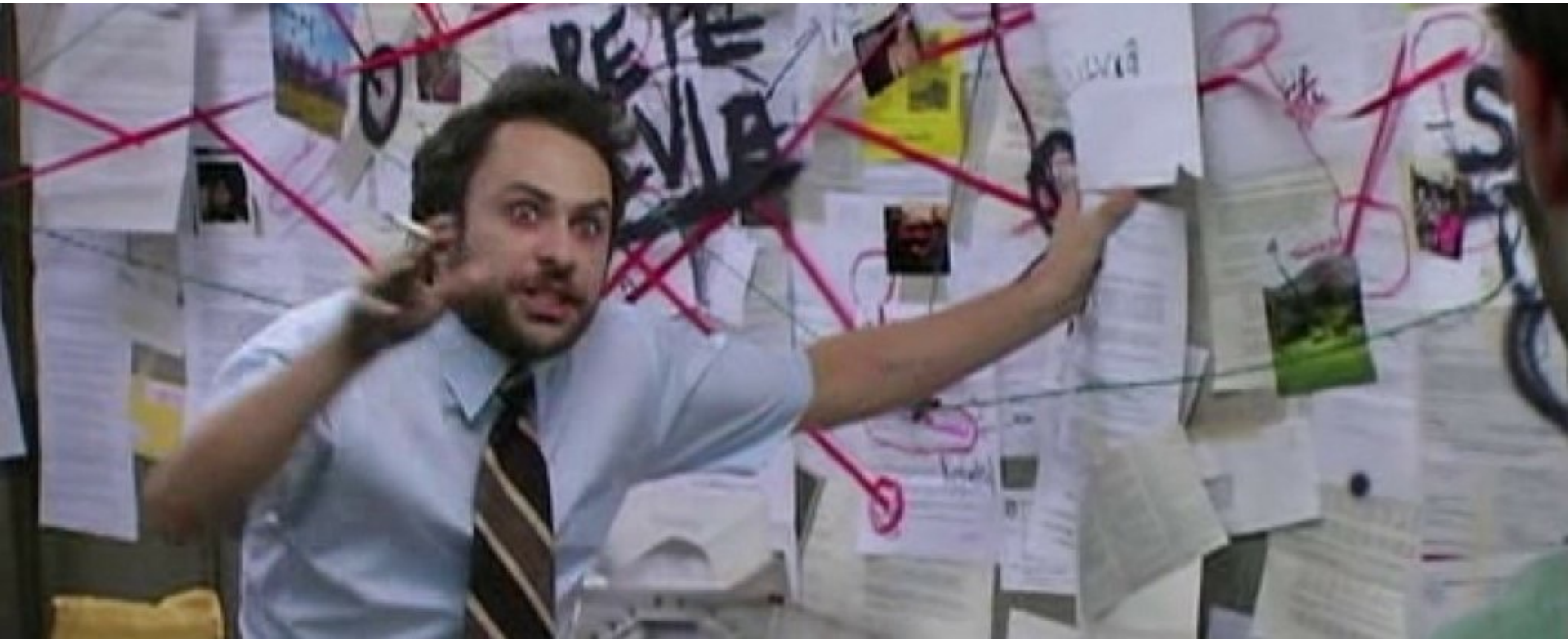

Airoha
(SoC, SDK, reference design)
We can search for these, but we will never find them all.
Vendor 1
Vendor 2
Vendor n
Vendor n+1
Vendor x
Product 1
Product 2
Product 3
Product 4
Product 5
Consumer


We might be able to identify and talk to a few of them.
Airoha
(SoC, SDK, reference design)
Vendor 1
Vendor 2
OEM/ODM 1
Vendor x
Vendor n
Vendor n+1
Product 1
Product 2
Product 3
Product 4
Product 5
Consumer

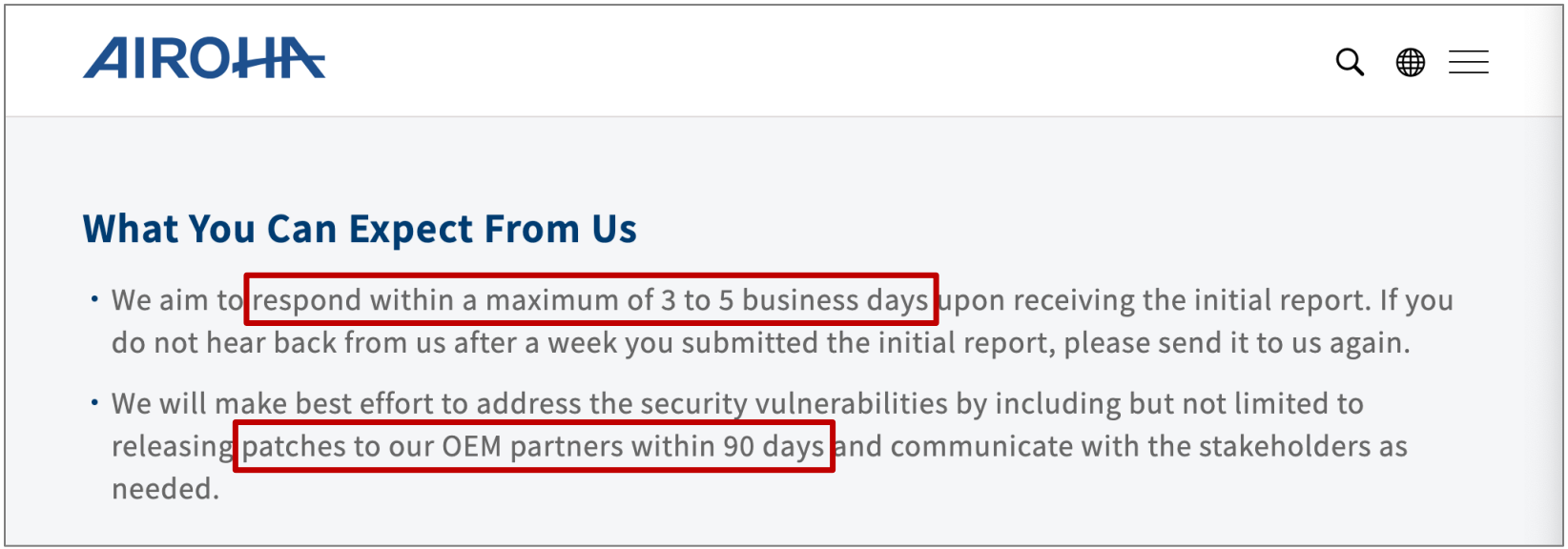

OEMs will also be difficult to identify.
Airoha
(SoC, SDK, reference design)
Vendor 1
Vendor 2
OEM/ODM 1
Vendor x
Vendor n
Vendor n+1
Product 1
Product 2
Product 3
Product 4
Product 5
Consumer

Our best chance is probably Airoha!

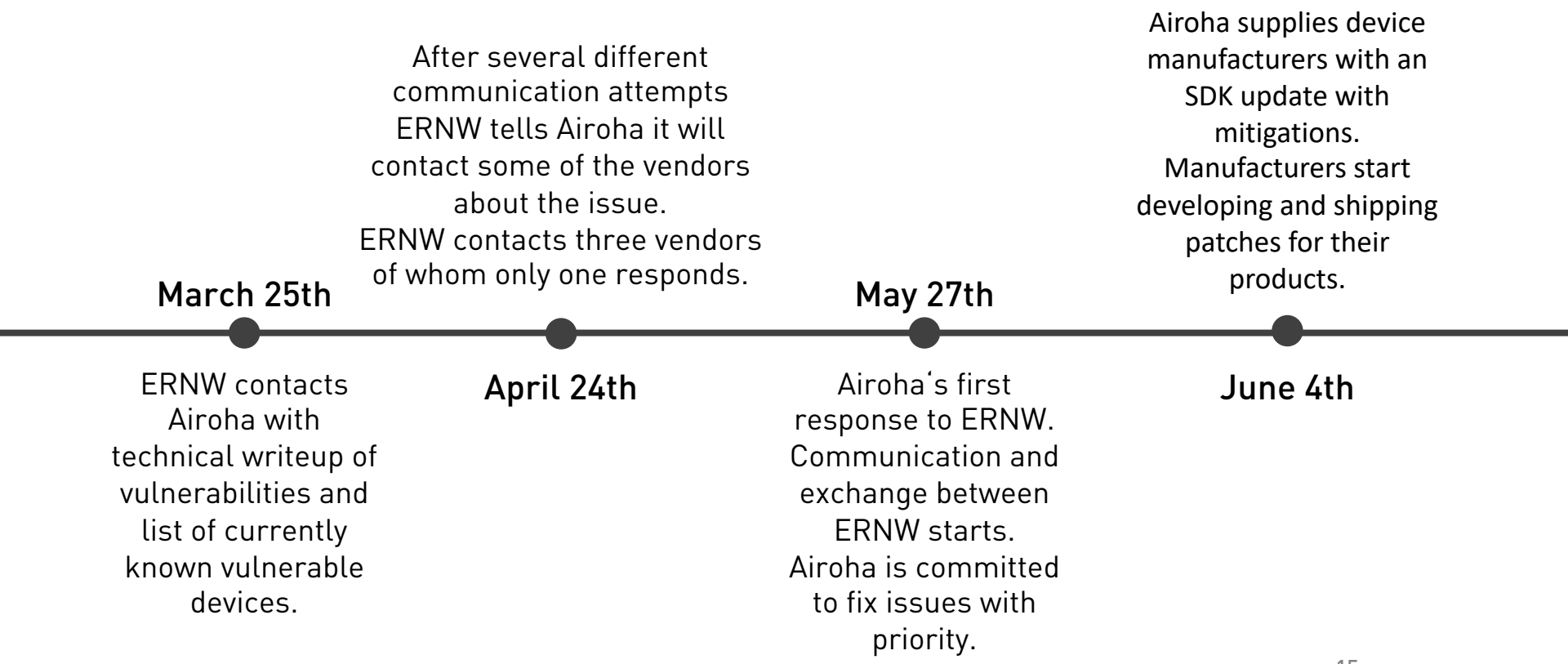




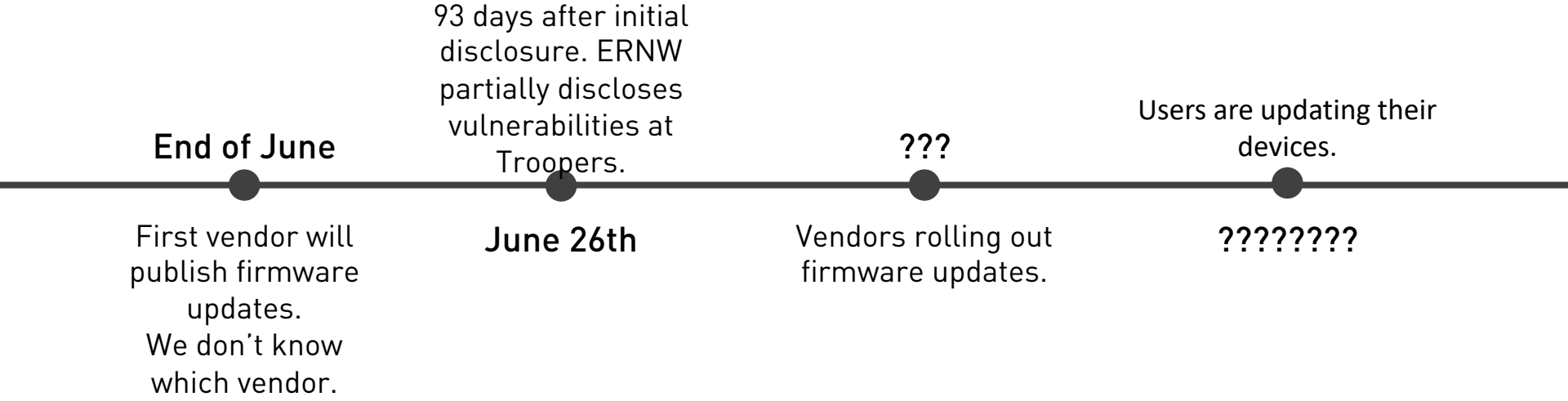
Airoha's security disclosure page looks really good!



Disclosure Timeline: **Short Version**



Disclosure Timeline: **Short Version**



Grundsätzlicher Ablauf

- Phase 1: Entdeckung & Dokumentation
- Phase 2: Kontaktaufnahme & Übermittlung von Details
- Phase 3: Koordination / Behandlung
- Phase 4: Abschluss & Veröffentlichung

Grundsätzlicher Ablauf

Einfachster Teil, Nicht Teil dieses Vortrags

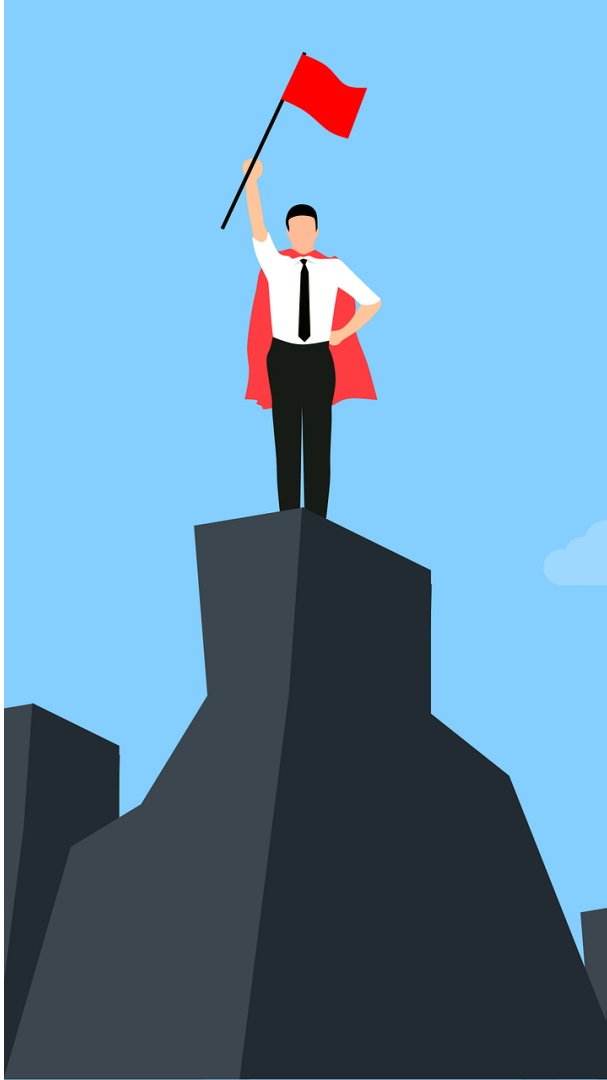
- Phase 1: Entdeckung & Dokumentation
- Phase 2: Kontaktaufnahme & Übermittlung von Details
- Phase 3: Koordination / Behandlung
- Phase 4: Abschluss & Veröffentlichung


Phase 2: Kontaktaufnahme &
Übermittlung von Details

Level 1: Einfach

- Vulnerability Disclosure Programme (VDP)
- RFC 9116: `/.well-known/security.txt`
- Vulnerability Disclosure Contact auf der Website des Unternehmens
- Incident-Kontakt des Unternehmens
- GitHub Issue Tracker, Mailing Lists

→ direkter Kontakt



Level 2: Mittel

- (Nicht-Security) Funktions-Mailadressen
  - Customer Support
  - Business Suport
  - Developer / API Support
  - GDPR- / DSGVO-Kontakt
  - Mailadressen aus öffentlicher Dokumentation
- Allgemeine Kontaktformulare

→ Suche nach einem geeigneten Kontakt

E-MAIL UNZUSTELLBAR

Diese E-Mail Kommunikationszeit ist abgelaufen und Ihre Nachricht kann nicht mehr erhalten werden.

Sehr geehrter Kunde,

Ihre Anfrage kann in Österreich nicht bearbeitet werden . Ausserdem fehlt die Sendungsnummer.

mfg

[redacted]

Hi there,

If this email is regarding a vulnerability report, we only accept reports via our Responsible Disclosure program: [redacted] If you have a vulnerability to report, kindly report it through that page.

Cheers,

Dear Ms. Suleder,

Thank you for contacting us.

Could you please share us the attachment again.

Level 3: Schwer

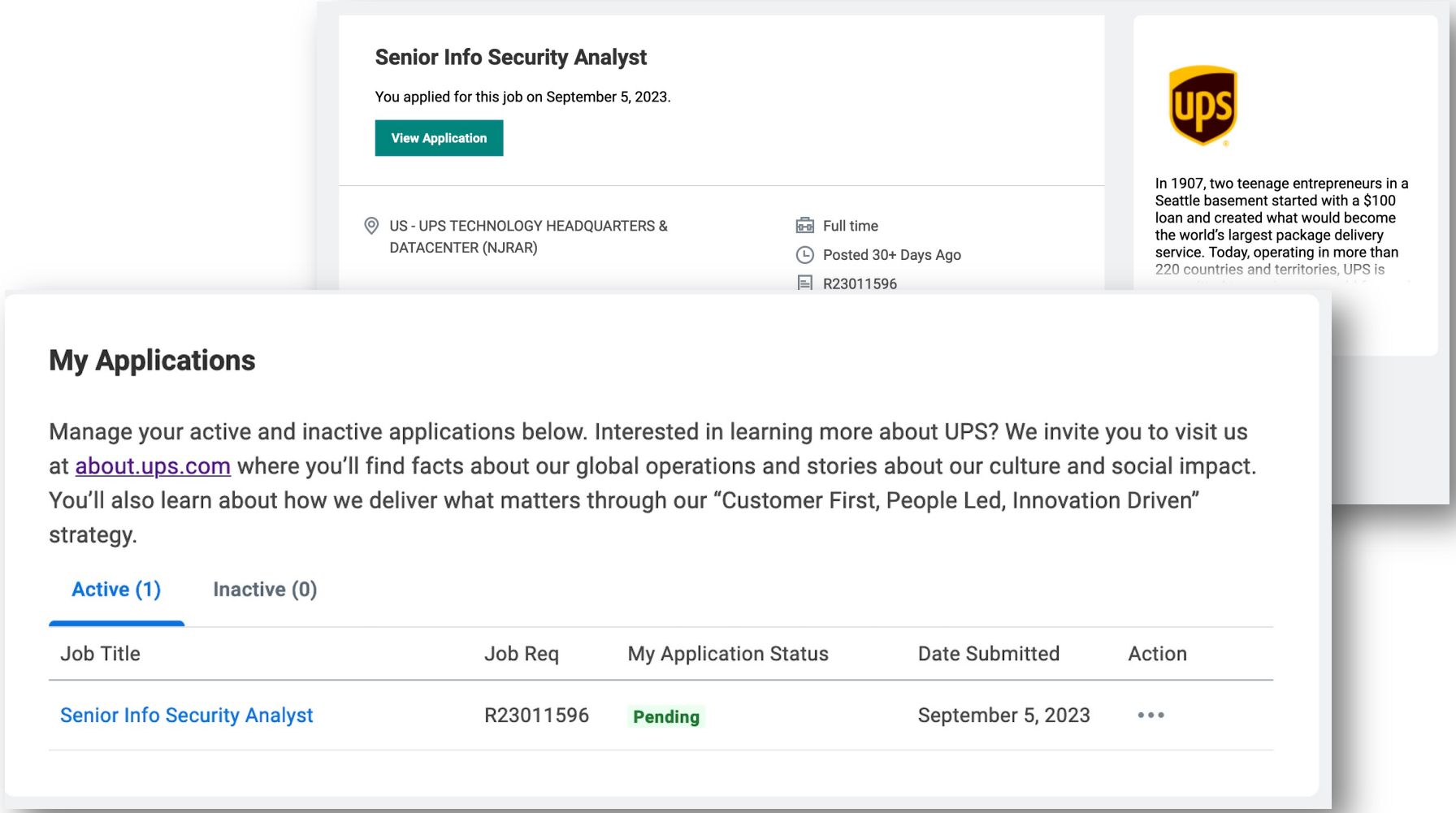
- Social Media:
  - X, Mastodon: Kennt jemand jemanden?
  - LinkedIn → IT Security bei $HERSTELLER
  - Persönliche Kontakte
- Bug Bounty Plattformen (z.B. HackerOne)

“Wir haben ein Bug Bounty Programm”

- **Bug Bounty Plattformen (BBP)**
  - Belohnen gezielt aktive Schwachstellensuche
  - Suche innerhalb definierter Scopes → gezielte und kontrollierte Analyse
  - Veröffentlichung der Schwachstelle nicht zwingend Teil des Programms
  - Externer Dienstleister → externer Prozess
- **Vulnerability Disclosure Programme (VDP)**
  - Offen für alle: Meldungen können von jeder Person eingereicht werden
  - Fokus auf Transparenz, Vertrauen und koordinierte Reaktion
  - Keine Limitation des Scopes → zum Zeitpunkt der Meldung „zu spät“
  - Integration in das interne Sicherheitsmanagement → Feedbackschleifen

Level 3: Schwer

- Social Media:
  - X, Mastodon: Kennt jemand jemanden?
  - LinkedIn → IT Security bei $HERSTELLER
  - Persönliche Kontakte
- Bug Bounty Plattformen (z.B. HackerOne)
- Stellenausschreibungen → Bewerben!


Senior Info Security Analyst
You applied for this job on September 5, 2023.
View Application
US - UPS TECHNOLOGY HEADQUARTERS & DATACENTER (NJRAR)
Full time
Posted 30+ Days Ago
R23011596
In 1907, two teenage entrepreneurs in a Seattle basement started with a $100 loan and created what would become the world's largest package delivery service. Today, operating in more than 220 countries and territories, UPS is
My Applications
Manage your active and inactive applications below. Interested in learning more about UPS? We invite you to visit us at about.ups.com where you'll find facts about our global operations and stories about our culture and social impact. You'll also learn about how we deliver what matters through our "Customer First, People Led, Innovation Driven" strategy.
Active (1)
Inactive (0)
Job Title
Job Req
My Application Status
Date Submitted
Action
Senior Info Security Analyst
R23011596
Pending
September 5, 2023


- First time?
- Huh?

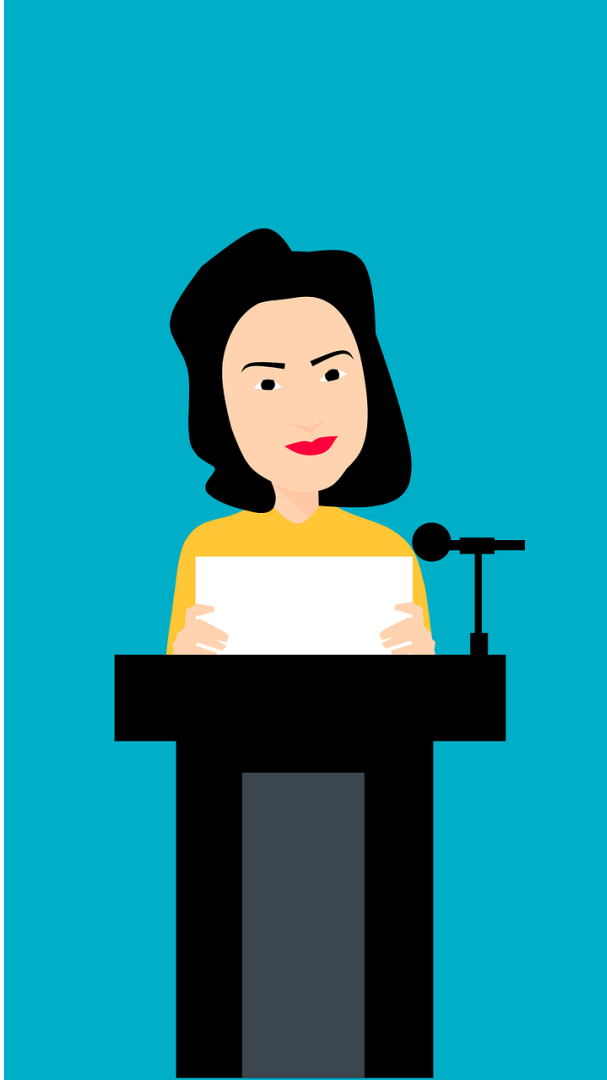
Phase 3: Koordination / Behandlung

Phase 3: Koordination / Behandlung

- Beispielhafte Aktivitäten:
  - Technische Diskussion der Findings
  - Diskussion von Maßnahmen
  - Diskussion einer Timeline für Fixes, Updates
  - Regelmäßige gegenseitige Updates
  - Später im Prozess: Koordination der Veröffentlichung
- Alle Aktivitäten sind abhängig vom Prozess
  - Transparenz des Herstellers / Einblicke in den Entwicklungsprozess
  - Kommunikationsverhalten
  - Direkte Kommunikation mit Fachabteilung oder Abstraktionslayer?
- Alle diese Dinge können sich im Laufe des Prozesses ändern!

Phase 4: Abschluss & Veröffentlichung

- Veröffentlichung von Details zur Schwachstelle
  - Anmeldung von CVEs
  - Advisory durch ein CERT
  - Talk auf einer Konferenz
  - Blog Post
  - Proof-of-Concept (PoC) Code
  - Berichterstattung durch Externe
- Problem:
  - Kundenanfragen / Außenwirkung?
  - Preisgabe von geistigem Eigentum?



Die Rolle von Bug Bounty Plattformen

Legal Notice:

If we conclude, in our sole discretion, that you have complied with the requirements above when reporting a security vulnerability, Sony will not pursue claims against you or initiate a law enforcement investigation in response to your report:

Disclosure Policy

- Please do not discuss this program or any vulnerabilities (even resolved ones) outside of the program without express consent from the organization.
- Follow HackerOne's disclosure guidelines.

- To the extent that you have accessed non-public Sony information in the course of your research, you do not maintain copies of any such information or share any such information with any third party; and
- You do not publicly disclose or share the vulnerability details without the written permission of Sony. Violation of these requirements may result in permanent disqualification from the program.

Landgericht Hamburg erlässt einstweilige Verfügung gegen IT-Sicherheitsfirma ERNW GmbH wegen Aufzeigen von Sicherheitslücken

Autor: Horst Speichert

Senior Partner

Rechtsanwalt

Veröffentlicht am 20.10.2015
unter #Allgemein

Die US-Sicherheitsfirma FireEye erwirkt vor dem Landgericht Hamburg eine einstweilige Verfügung (312 O 357/15) gegen unsere Mandantin die ERNW GmbH aus Heidelberg, weil sie Sicherheitslücken in einem Softwareprodukt von FireEye aufgezeigt hat. Obwohl die ERNW GmbH die Bekanntgabe der Sicherheitslücken in einem „Responsible-Disclosure-Verfahren" mit FireEye abgestimmt hat, wurde eine einstweilige Verfügung vor dem Landgericht Hamburg erwirkt. FireEye steht wegen dieses unangemessenen Umgangs mit den Sicherheitsexperten der ERNW GmbH aktuell in den Medien stark in der Kritik. Rechtsanwalt Speichert aus der Kanzlei esb Rechtsanwälte in Stuttgart vertritt die ERNW GmbH vor dem Landgericht Hamburg.

Quelle: https://www.kanzlei.de/landgericht-hamburg-erlaesst-einstweilige-verfuegung-gegen-it-sicherheitsfirma-ernw-gmbh-wegen-aufzeigen-von-sicherheitsluecken


SHHH NO MORE TALKING
imgflip.com

Phase 4: Abschluss & Veröffentlichung

- Kontextuelle Lücken // Missing Link:
  - Wenig Einblick in das Unternehmen
    - Organisationsstruktur & (Fehler-)Kultur
    - Eigene Abteilung für Security Reports?
    - Firmenpolitik Innen & Außen
      - → Jedes Unternehmen agiert in einem Kontext
      - → Selten ist dieser Kontext von außen deutbar
  - Komplexität durch Produkt, Branche, Regulatorik:
    - Medizinprodukt vs. mobile App
    - Open Source Software

Beispiel 1: Rigide Prozesse

Disclosure Timeline

- February 04, 2025: Initial contact attempt by ERNW via Mail stating it cannot accept the terms and conditions of HackerOne .
- February 10, 2025: Contact attempt by ERNW.
- February 11, 2025: Contact attempt by ERNW.
- February 11, 2025: PagerDuty Security Team states only reports via HackerOne are accepted.
- February 12, 2025: ERNW states it cannot accept the terms and conditions.
- February 14, 2025: Contact attempt by ERNW.
- February 26, 2025: Contact attempt by ERNW.
- March 04, 2025: Contact attempt by ERNW.
- March 27, 2025: Contact attempt by ERNW.
- May 05, 2025: Contact attempt by ERNW stating that the disclosure timeline is exceeded. Public Disclosure by ERNW.

Quelle: https://insinuator.net/2025/05/full-disclosure-multiple-rundeck-job-command-injections/

Beispiel 2: Kommunikation > /dev/null

Disclosure Timeline

- May 11, 2023: Initial contact to UPS, start of 90-day disclosure period.
- June 01, 2023: New contact attempt.
- September 05, 2023: New contact attempt.
- September 07, 2023: First reaction by a UPS "fraud mitigation analyist" asking us to resend some attachments.
- September 08, 2023: All information is sent again to this contact person.
- September 14, 2023: New contact attempt because no follow-up reaction by UPS.
- September 26, 2023: New contact attempt.
- October 04, 2023: New contact attempt.
- October 31, 2023: New contact attempt.
- November 14, 2023: New contact attempt.

Quelle: https://insinuator.net/2024/04/breaking-ups-parcel-tracking/

Beispiel 2: Kommunikation > /dev/null

Disclosure Timeline

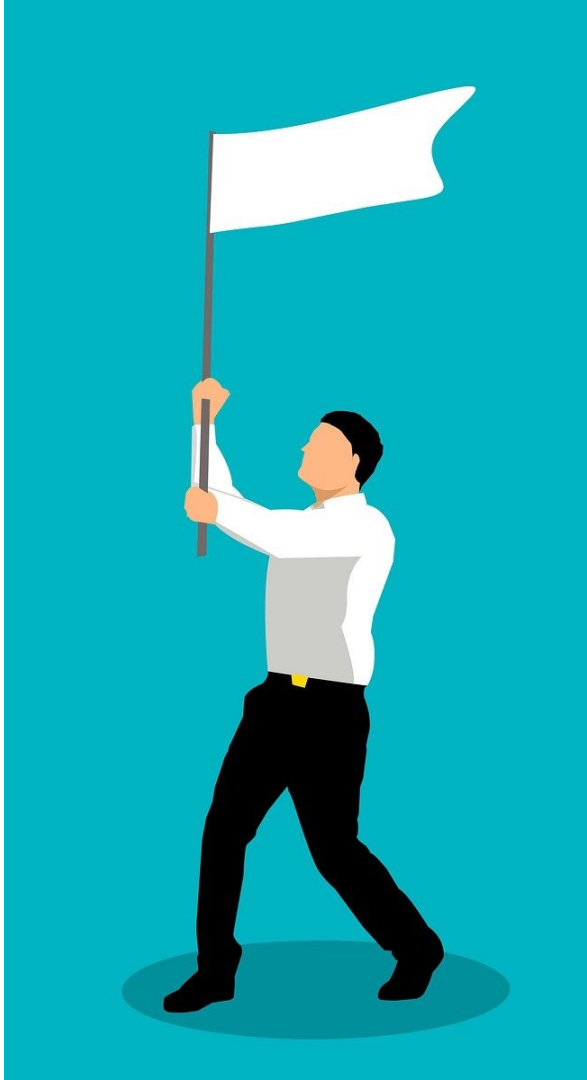
- November 20, 2023: New contact attempt.
- January 08, 2024: New contact attempt.
- February 02, 2024: ERNW decides to report the vulnerabilities to the Cybersecurity & Infrastructure Security Agency (CISA) which is part of the U.S. Department of Homeland Security. Handling software vulnerabilities is managed by Carnegie Mellon University's CERT Coordination Center (CERT/CC).
- February 19, 2024: ERNW requests CERT/CC for coordination assistance and submits a detailed vulnerability report.
- February 26, 2024: The CERT decides not to handle the case.
- March 19, 2024: ERNW decides to fully disclose the vulnerabilities.
- April 10, 2024: Publication of this blog post.

- November 14, 2023: New contact attempt.

Quelle: https://insinuator.net/2024/04/breaking-ups-parcel-tracking/

Ergebnis: Aufgeben

- >50 Kontaktaufnahmeversuche per Mail
- >15 LinkedIn Kontaktaufnahmeversuche
- 2 erfolglose Bewerbungen
- Ablehnung des Falls durch ein CERT
- Nach Konsultation unseres Ethik-Komitees
- → Full Disclosure nach 11 Monaten



Geht der Trend zum Full Disclosure?

Geht der Trend zum Full Disclosure?

- Full Disclosure bedeutet:
  - Die vollständigen technischen Details der Schwachstelle werden ohne vorherige Koordination öffentlich gemacht.
- Mögliche Gründe für den Verzicht auf ein Coordinated Disclosure
  - Kontaktversuche: Keine Reaktion vom Hersteller
  - Blockade oder Ablehnung, Schwachstelle “Out-of-Scope” / nicht valide
  - Unverhältnismäßige Verzögerung oder Stille: Einseitige Kommunikation
  - Rechtliche oder kommunikative Eskalation
- Sozusagen: „Die Reißleine Ziehen“
- Problem: Es gibt keinen Fix, Schwachstelle exploitbar → Risiko?
- Milderes Mittel: Übertragung des Prozesses an ein CERT


Und jetzt?
Wie geht es weiter?

Vulnerability Reporting Best Practices & Prozesse

- Was ist das Ziel, des Sicherheitskontakts/Meldeverfahrens?
  - → vertrauenswürdiger Kanal für Meldungen
  - → Demonstration, dass Meldungen ernst genommen werden
- Vorbereitung, Vorbereitung, Vorbereitung
  - Definition von Regeln für den Prozess für interne und externe Parteien
    - Der Prozess sollte so offen wie möglich sein
    - Aufzeigen, was von Ihnen als Hersteller/Betreiber zu erwarten ist
  - Integration der Meldungen in relevante Prozesse → Kultur
  - Kommunikation auf Augenhöhe → „Don't shoot the messenger“
- Es wird immer Ausnahmen geben → Kommunikationskanäle!
- Schwachstellen in Third-Party Software sollten gemeldet werden!

Literatur & Referenzen

- ISO/IEC 29147:2018: Informationstechnik - Sicherheitstechniken - Offenlegung von Schwachstellen
- ISO/IEC 30111:2020: Informationstechnik - IT-Sicherheitsverfahren - Prozesse für die Behandlung von Schwachstellen
- RFC9116: A File Format to Aid in Security Vulnerability Disclosure
- FIRST Multi-Party Coordination and Disclosure
- OWASP Vulnerability Disclosure Cheat Sheet
- Carnegie Mellon University / CERT CC: The CERT Guide to Coordinated Vulnerability Disclosure

Danke für die Aufmerksamkeit!

Kontakt via jsuleder@ernw.de oder LinkedIn