TLP:CLEAR

○○○

Software Dependency Failures

jQuery, a Canary in the Coal Mine

Lari Huttunen

2023-10-05

OOPSIE

= **O**utrageously **O**dd **P**roblems and **S**ecurity **I**ssues **E**xamined

- Internal Arctic Security research project started in 2018.
- Heavy focus on uncovering systemic issues on the Internet.
  - One of the main ingredients for the Arctic NCSC feed.
- Some of the research results published on Public Exposure.
  - (An independent blog on cyber security.)

Terminology

Deductive reasoning:

- Deductive reasoning starts with a general premise or statement and draws a specific conclusion from it.

Inductive reasoning:

- Inductive reasoning involves making generalizations or predictions based on specific observations or evidence.

Abductive reasoning:

- Abductive reasoning seeks to find the best possible explanation for a set of observations or evidence.

My Canary: CVE-2020-11022

In jQuery versions greater than or ***equal to 1.2 and before 3.5.0****, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is* ***patched in jQuery 3.5.0****.*

https://nvd.nist.gov/vuln/detail/CVE-2020-11022

TLP:CLEAR

Is it exploitable?

The Key Here is Obsolescence

- Is the host operating system EOL?
- Does the host suffer from public exposure?
- Are the service components up-to-date?
- Are there other vulnerabilities within the host?
- What does the organization’s security posture look like?

Context: jquery-ui as a Marker

- Why jquery-ui?
  - A set of interactive widgets.
  - More likely to have login forms.
- jquery-ui depends on jquery
- The research subject population: ~1.8m hosts
- Shodan dork:
  cpe:/a:jquery/jquery_ui

TLP:CLEAR

DEMO Ingredients

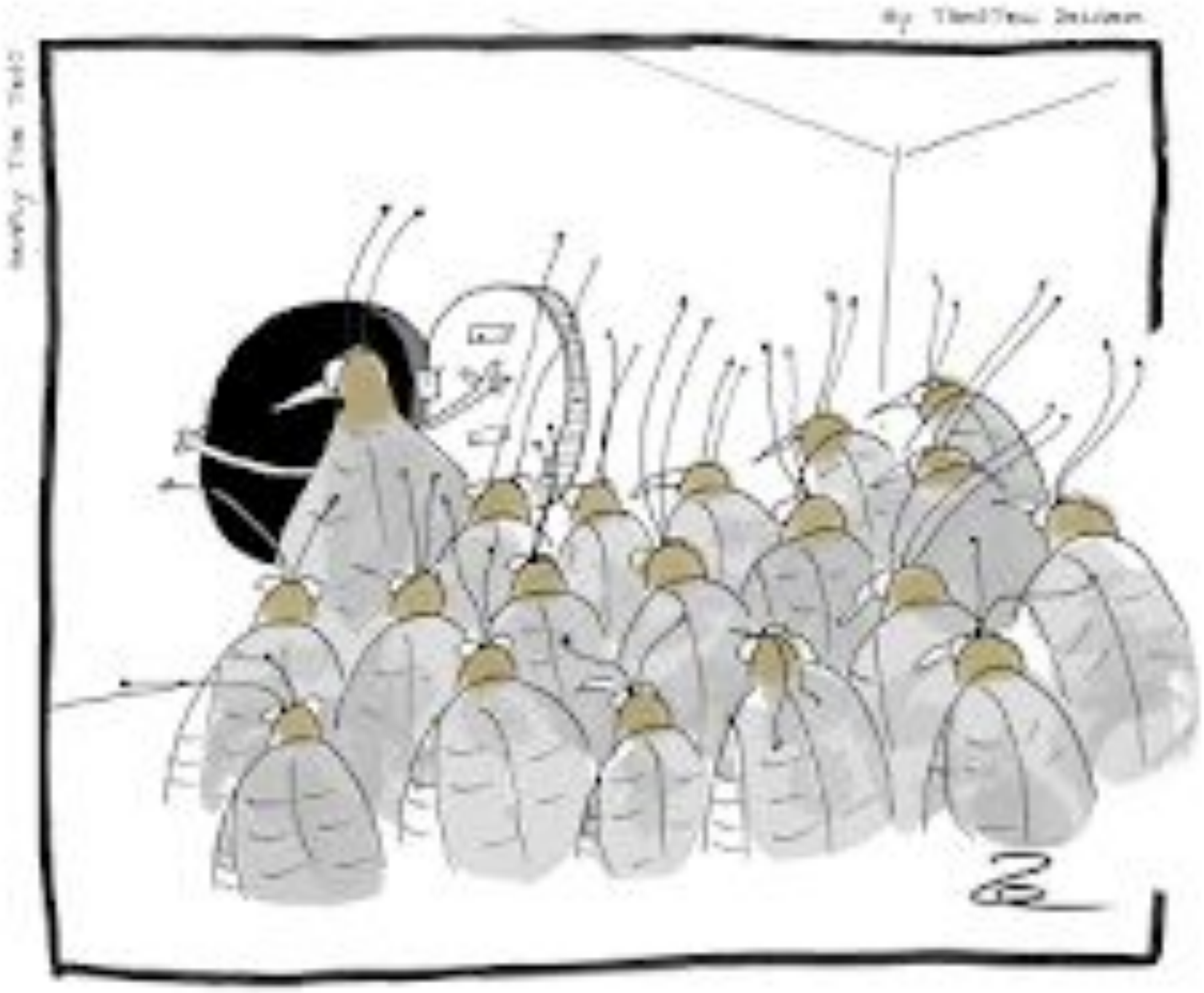
- Arctic NCSC feed (observations)
  - ~200 feeds based on OOPSIE research.
- Arctic HUB (+ other internal tools)
  - To demonstrate the problems (in Latvia).
- Shodan (for more contextual cues)
  - To look at a given host in a bit more detail.
- Lookyloo (to have a peek)
  - To take a peek at the web service behind a given IP.
- Chat GPT (maybe)
  - For *shits and giggles*, err, context.

DEMO Flow

component -> service -> host -> organization

TLP:RED

On to the DEMO (Effects)



"Hang on, the demo starts soon, then let's go out and ruin their show".

Solution for Software Dependency Failures?

- **Dependendabot**
  - https://github.com/dependabot
  - Solves the problem only for software developers.
- **For sysadmins?**
  - SBOM gives and idea of the current state of affairs.
  - How to track over time?

TLP:CLEAR

Thank You!

- Further reading: https://public-exposure.inform.social/post/software-dependency/
- Write for us! :) https://public-exposure.inform.social/write-for-us/