



IT Security 2024/2025

Exercise Sheet 11

– Supply Chain Attacks –



Dr. Marc Ohm

Publication: 18.12.2024
Deadline: 08.01.2025 10:00



Lightning Survey ⚡

Exercise 1 (Intrusion Kill Chain for event-stream, 2 points). Provide a brief, concise description (2 sentences maximum) of each step in the intrusion kill chain for the software supply chain attack using `event-stream`. Write your solution into `event-stream.txt`.

Exercise 2 (Analyze Malicious Package, 3.5 points). Analyze the malicious package `browserift` (already in your repo) to answer the following questions:

- What triggers the execution?
- Is it specific to a certain operating system? If yes, which and why?
- What obfuscation technique is used to hide the malicious code?
- What is the objective of the attack?
- How is that objective achieved, i.e. implemented?
- What was the attack vector?
- What is the latest version of the package in the `npm` package registry?

We've disarmed crucial parts, but you probably shouldn't run it anyway. Write your solution into `browserift.txt` with no more than a line per subtask.

Exercise 3 (Capture the Flag using a malicious Package, 4.5 points). Write a proof of concept package that is able to exfiltrate a certain environment variable (flag) of the submission pipeline. Craft an npm (JavaScript/Node.js v12) package¹ named `poc-itsec` and version `1.0.0`. When done, create a tarball using `npm pack`. We will install your package using `npm install poc-itsec-1.0.0.tgz` and subsequently execute the main script using `node ./node_modules/poc-itsec`. But be aware that we have implemented rudimentary detection capabilities! Check the pipeline output to validate your solution and make sure the value of the flag `ITSEC{...}` is visible on stdout.

¹<https://docs.npmjs.com/creating-node-js-modules>