Challenge #4
Analyze a security advisory

Anchoring and overview

Modul:	679	Informationen über Bedrohungen beschaffen und aufbereiten
Handlungsziele:	HZ 1	Beschafft laufend, proaktiv und selbstgesteuert Informationen über aktuelle Bedrohungen im Cyber-Raum.
Modul:	685	Schwachstellen- und Patchmanagement im Betrieb sicher-stellen
Handlungsziele:	HZ 1	Überwacht die aktuellen Entwicklungen bezüglich Schwach-stellen im operativen Betrieb laufend.
Leistungskriterien PO:	LK-A-1	CSS können verschiedene Informationsquellen zu Bedrohungen zu unterscheiden.
	LK-A-8	CSS können geeignete technische oder organisatorische Schutzmassnahmen zu definieren und umzusetzen.
	LK-C-4	CSS können technische Sofortmassnahmen situations- und kontextspezifisch auszuwählen, zu implementieren und in Bezug auf die Wirksamkeit zu überprüfen

Formulation of task (candidate view)

Analyze a security advisory

Resources

[1] Vulnerability Note VU#930724, Apache Log4j allows insecure JNDI lookups, Carnegie Mellon University CERT, https://www.kb.cert.org/vuls/id/930724

Introduction

On a Friday morning, Swiss National Cyber Security Centre (NCSC) receives reports about a critical vulnerability in a popular Java library called *"Log4j"*. At the time of receiving these reports, the vulnerability apparently is exploited by threat actors "in the wild" and no patch is available to fix the vulnerability (0-day exploit).

You are security analyst in a large company's Security Operation Center (SOC) and soon as you got the security advisory forwarded, you receive already questions about the new vulnerability from concerned colleagues. The operation manager scheduled a meeting to discuss the situation for the company and action needs. You will be asked to present an overview about the vulnerability and the threat to the company.

Goal and tasks

To be prepared for the meeting, perform an analysis of the given security advisory and work out the following five topics in a written report:

1. Sketch a **pictural overview** how the log4j attack works (so that you would be able to present an attack overview on a flipchart in the meeting).
2. Give a description of the **problem**(s) of the log4j attack, why is it rated critical.
3. **Relevance** for the company: Describe why this attack is relevant for the company.
4. **Challenges**: Describe three different challenges that make it difficult to solve the problem.
5. **Next steps**: Describe three different organizational or technical steps to tackle the problem.

Submission

Submit a written report as a PDF document, containing the information structured as outlined in the goal and tasks section.

Specifications for correction

Evaluation criteria

Attack overview

C01: Pictural attack overview correct and understandable (useable as a basis to be reproduced at a flipchart in the meeting) = 3 pt.

Problem description

C02: Problem description contains aspect of remote exploitation = 1 pt.

C03: Problem description contains aspect of unauthenticated actions = 1 pt.

C04: Problem description contains aspect of arbitrary code execution = 1 pt.

Relevance

C05: Distribution recognized and described understandable = 3 pt.

Challenges

C06: Challenge correct, specific, understandable and comprehensible = 1 pt.

C07: Challenge correct, specific, understandable and comprehensible = 1 pt.

C08: Challenge correct, specific, understandable and comprehensible = 1 pt.

Next Steps

C09: Action understandable, specific and comprehensible = 1 pt.

C10: Action understandable, specific and comprehensible = 1 pt.

C11: Action understandable, specific and comprehensible = 1 pt.

Correction instructions

- This challenge gives a maximum of **15 points**.
- Given scores on the criteria may not be further subdivided.
- Challenges & Next steps: If a solution contains more than 3 options, only the first 3 are assessed!

Sample solutions

The analysis has to contain the following information:

Attack #1	
Attack overview	Provide a simple explanation of an attack flow, in picture such as Zero-Day Exploit Targeting Popular Java Library Log4j (admin.ch)
Problem description	The vulnerability is critical, as it can be **exploited from remote (C02)** by an **unauthenticated (C03)** adversary to **executed arbitrary code (C04)** (remote code execution – RCE).
Relevance #2	
Distribution	Log4j is a **popular Java library** developed and maintained by the Apache foundation. The library is **widely adopted** and **used in many commercial and open-source software products** as a **logging framework** for Java.
Challenges #3	
Challenge	Inventory Many companies have **weak asset management** processes, so it is hard to figure out where the software is used
Challenge	Responsibility Often asset **ownership** is not defined, so the administrators that can implement immediate measures or patch solutions are not known
Challenge	Suppliers and third-party management **Products delivered by suppliers** and/or **managed by third parties** have to analyzed also, information gathering and measure application (e.g. patching) has to be coordinated
Challenge	Communication **Weak credential management**, an attacker becomes aware of valid credentials of a Windows end-user system, e.g. password leaks
Next steps #4	
Action	Make a **risk assessment** and define the company's **target**
Action	**Plan** your actions and define the essential **team** that has participate and their roles
Action	Clearify **patch availability** for your affected products
Action	Provide **self-service tools**, easy to use scripts for vulnerability discovery (scanner) and/or patching of systems