Log4Shell from the inside

Annika Andreasson
Center for Security and Resilience
Stockholm School of Economics

CDIS Spring Conference
May 21, 2026

Log4Shell from the inside

Andreasson, A., Artman, H., Brynielsson, J., & Franke, U. (2025).
Cyber situation awareness during an emerging cyberthreat: A case study.
International Journal of Information Security, 24(5), 217.

Software

This article is more than 4 years old

Recently uncovered software flaw 'most critical vulnerability of the last decade'

Log4Shell grants easy access to internal networks, making them susceptible to data loot and loss and malware attacks

Associated Press

Sat 11 Dec 2021 02.50 CET

Cybersecurity experts say Minecraft players have already exploited a software flaw to breach other users by pasting a short message in a chat box. Photograph: Damian Dovarganes/AP

A critical vulnerability in a widely used software tool - one quickly exploited in the online game Minecraft - is rapidly emerging as a major threat to organizations around the world.

"The internet's on fire right now," said Adam Meyers, senior vice-president of intelligence at the cybersecurity firm Crowdstrike. "People are scrambling to patch", he said, "and all kinds of people scrambling to exploit it." He said on Friday morning that in the 12 hours since the bug's existence was disclosed, it had been "fully weaponized", meaning malefactors had developed and distributed tools to exploit it.

The flaw, dubbed "Log4Shell", may be the worst computer vulnerability discovered in years. It was uncovered in an open-source logging tool, Log4j, that is ubiquitous in cloud servers and enterprise software used across the industry and the government. Unless it is fixed, it grants criminals, spies and programming novices alike, easy access to internal networks where they can

Israeli spyware firm targeted Apple devices via iMessage, researchers say

Read more

Most viewed


Workers racing to turn reflecting pool blue for Trump may be at risk, union warns


Live
Manchester United v Nottingham Forest: Premier League – live


'It's no longer exceptional': Karachi struggles under brutal new reality of extreme heat


It may not feel like it, but hope is on the horizon: Trump, Netanyahu and Putin's powers appear to be waning
Simon Tisdall


Trump news at a glance: billions of taxpayer dollars could go to president and his allies in unprecedented move

Research question

RQ: What challenges do staff involved in cybersecurity work in a large, complex organization experience when developing cyber situation awareness while handling an emerging cyberthreat?

Sub-questions:

- How did information about the emerging cyberthreat spread to staff involved in the handling of the threat throughout the organization?
- What common operational pictures existed to aid staff cyber situation awareness while handling the emerging cyberthreat?
- What were the staff experiences of information sharing for cyber situation awareness during the handling of the emerging cyberthreat?

The organization

- Large, complex organization with subsidiaries and several administrative departments.
- Primary mission is to deliver essential public services and critical infrastructure.
- General IT services are provided to parts of the organization by a Service department with an Incident manager function.
- There is also an organization-wide, separate CISO function with a CERT.

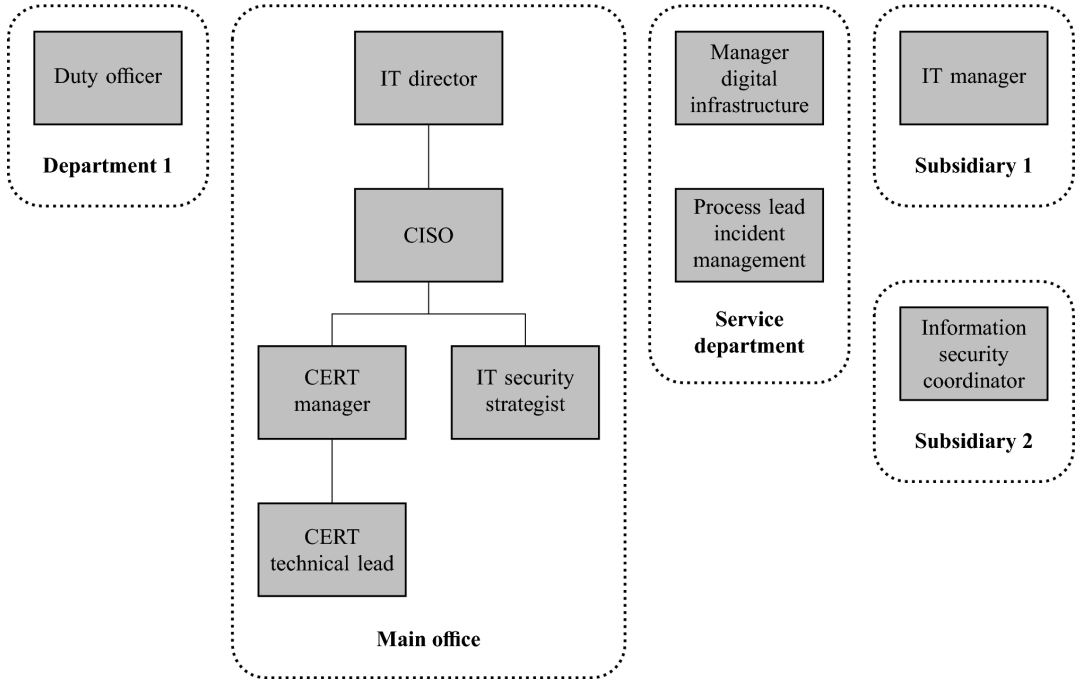
Case study

Data collection:

- Semi-structured interviews
  - 10 members of staff
    - 4 initial sample
    - 6 snowball sample
- Documents
  - CERT common operational pictures
  - CERT emails
  - Timelines created post incident
  - Timelines from CERT lessons learned report

Participants & organizational context

	No.	Role	Years in role
Initial	1	IT security strategist	5
	2	CERT manager	3
	3	CERT technical lead (*C*)	3
	4	CISO	9
Snowball	5	IT director	10
	6	IT manager (acting CIO) (*S*)	6
	7	Information security coordinator (*S*)	5
	8	Process lead incident management	3
	9	Manager digital infrastructure	2 months
	10	Duty officer	6



How the event unfolded...

Calm before the storm

2021-12-09 Thursday

- *CERT technical lead* hears about a possible vulnerability from an external colleague.

2021-12-10 Friday

- CERT receives additional information from trusted external sources stating that the vulnerability might be rated “critical”.
- CERT analysts feel compelled to issue a CERT message stating that there is a critical vulnerability in the Java library Log4j and instructions on mitigation.

Red alert—Gale and dark skies

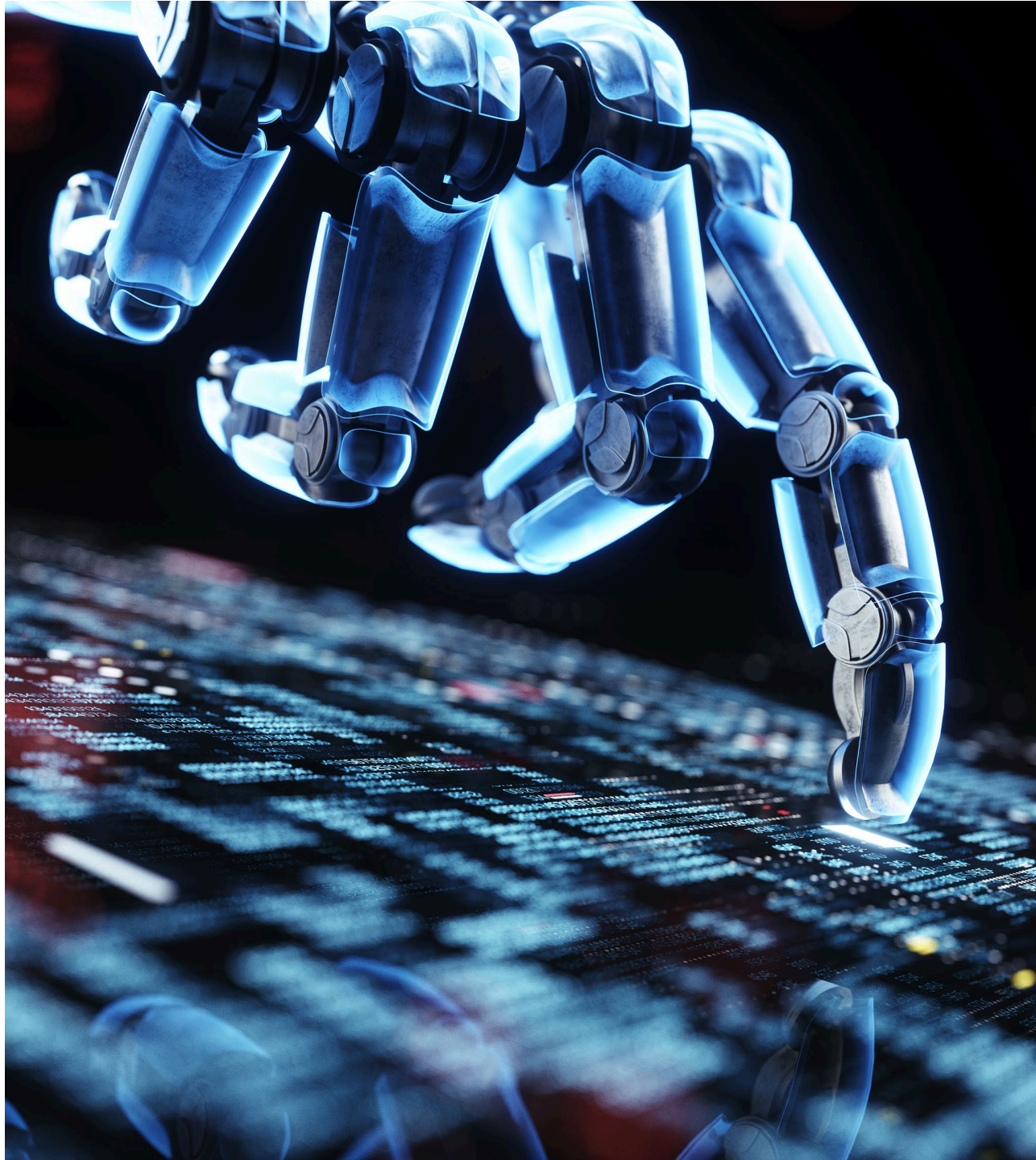
2021-12-11 Saturday

- A couple of informants are reached by different external sources. A service provider calls *CISO and IT director* and calls to a meeting with similar organizations nationwide.
- The supplier says that the vulnerability ”has been exploited”.
- CERT activates the standard operating procedure for anomalous events.
- *Manager digital infrastructure* signs a contract with a private cybersecurity firm.
- *CERT technical lead* starts checking logs and setting up alerts for attacks
- *Duty officer* is called by *CISO* or a member of the CERT and made aware of a potentially serious situation.
- Media reports “the Internet is on fire”.

All hands on deck

2021-12-12 Sunday

- *Process lead incident management* leads a task force meeting at 10:00. *CERT manager*, *CISO*, *IT manager*, *Information security coordinator*, and *Manager digital infrastructure* all participate
- Service department starts server inventory creating lists of servers with the vulnerable Log4j version to be checked
- CERT begins vulnerability scans



What’s going on?

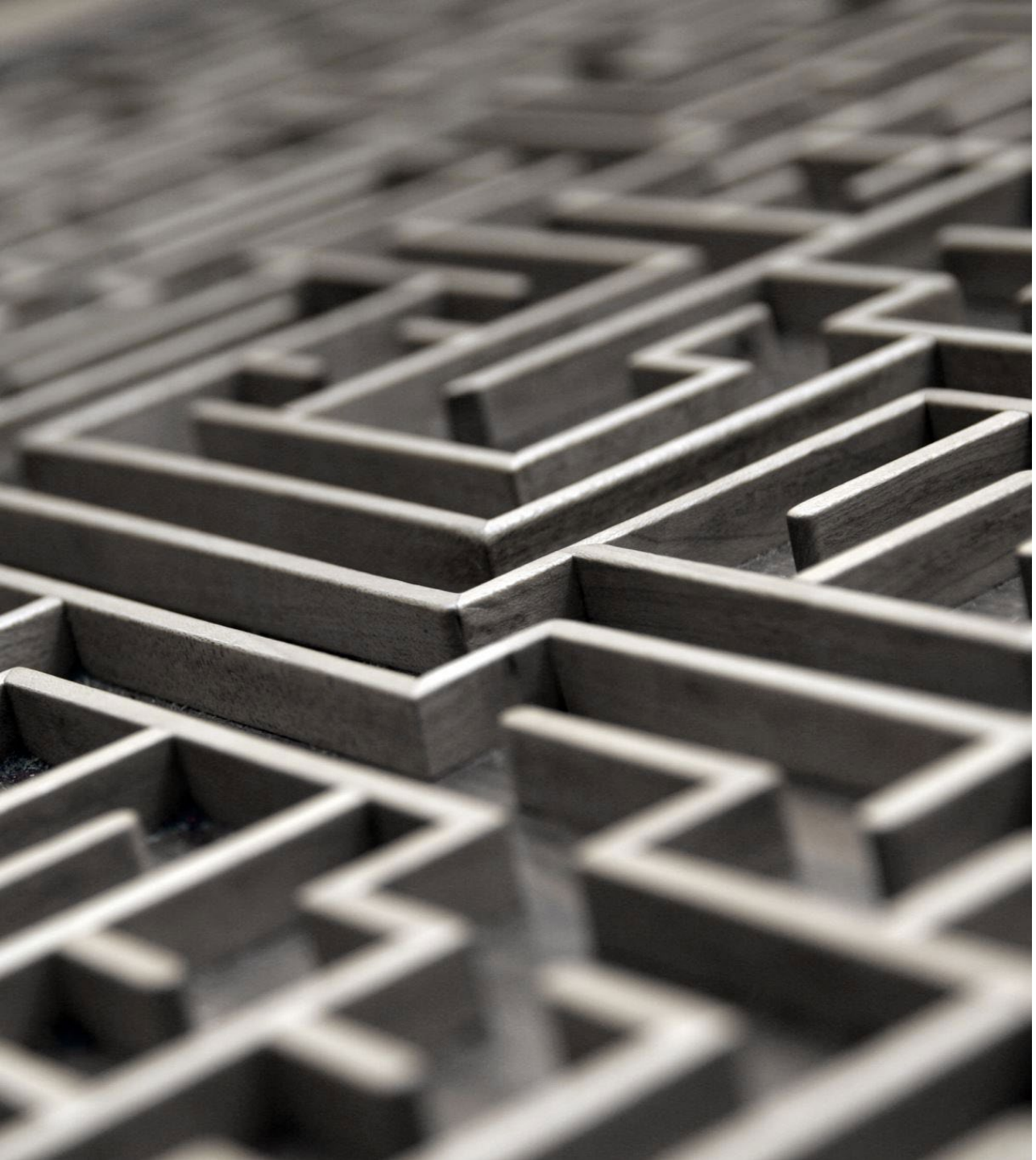
2021-12-13 Monday

- CERT follows their SOP and starts battle rhythm meetings 4 times daily and establishes common operational pictures (COP) at each meeting. First meeting at 09:00.
- IM holds task force meeting at 10:00.
- CERT retracts previous advice on mitigation as more versions found vulnerable.
- Common operational pictures from the CERT are adapted to be passed on in the chain *CERT manager – CISO – IT director.*

Ebbing out

2021-12-14 Tuesday and onwards

- Subsidiary 2 are done wtih their vulnerability scans – nothing found.
- *CERT manager* finds out that there was a miscommunication with the supplier affected by the vulnerability. The supplier had the vulnerability in their system, but it was never exploited
- *CISO*'s heightened alert recedes as no evidence of exploitation have been found.
- IM's checked systems list is growing longer .
- *IT director* deprioritizes national meetings and sees a shift from the vulnerability being "the end of the world" to them knowing what's going on and being able to handle the event as a regular vulnerability.



Challenges during the incident

- Absence of an organization wide common operational picture
- Inaccurate information being shared
- Information sharing among staff was not without effort
- Cyber situation awareness was fragmented.

THANK YOU!

Annika.Andreasson@hhs.se

Stockholm School of Economics | Box 6501 | SE-113 83 Stockholm | +46 8 736 90 00