Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Reflections on spearheading the community effort on sharing Log4j information via Github

NCSC-NL

66th TF-CSIRT Meeting, May 2022

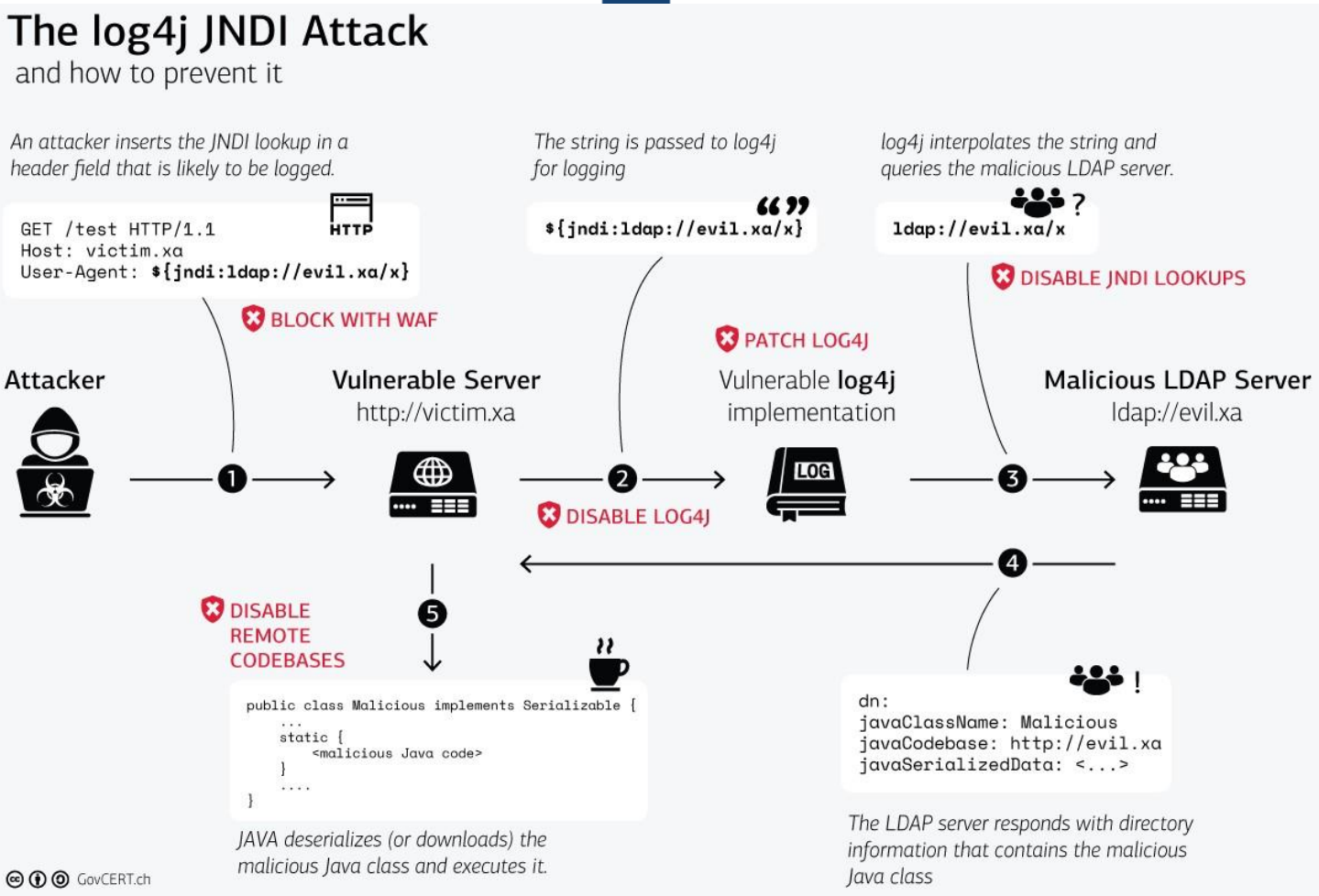
NCSC

Contents

- Log4shell
- Overview of NCSC-NL activities
- Github Repo
- Success / Issues
- International collaboration
- Future

The log4j JNDI Attack

and how to prevent it



Log4J: Overview of activities

Dedicated Log4j team active since 11 December on a rotating basis responsible for monitoring, planning and execution.

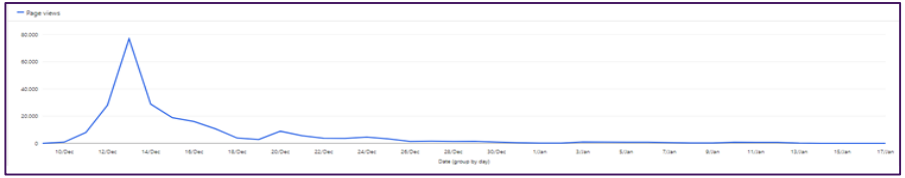
Key activities:

- Daily meetings to assess the situation and plan for action
- Update our Log4j advisory
- Communicate to our constituencies on new vulnerabilities, patches, mitigation measures, IT/OT, scenarios and current threat intel
- Organize meetings with our constituencies and third parties.
- Ensure policymakers were properly informed
- Broad outreach through media, Twitter and website

- Maintaining Github

Page views ncsc.nl/log4j

Page views	Unique page views	Entries	Page bounce rate	Average time on page	Exit rate
239.657	195.128	153.001	74,57%	57s	91,08%



Media outreach

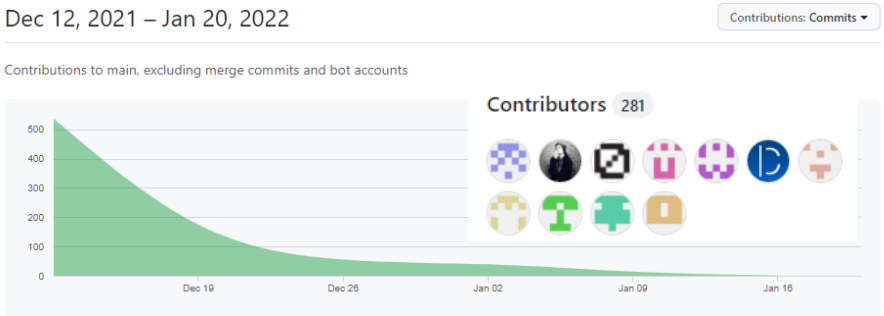
Log4J: Github repo

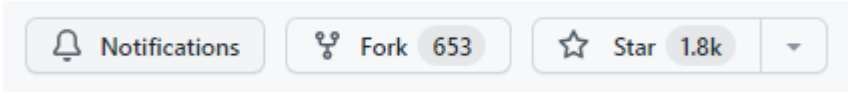
A lot of pieces to the puzzle!

- We did not have unique information position based our own expertise
- Log4shell were vulnerabilities with a lot of pieces of information everywhere

One of the first actions taken by NCSC-NL

- Lot of requests for single list of vulnerable software.
- Continues updating not possible through usual comm channels.
- Operational information harder to summarize on conventional platforms





Over 2m views and 600k unique visitors in first week alone

Log4J: Github repo (Success / Issues)

Success

- Wide adaption due to backing of National CERT.
- NCSC-NL can support repo 16/7
- Widespread adaption ensured many contributions from security experts, commercial organizations.
- Familiarity with git/Github enabled 3rd parties and CERT's to make contributions
- Github actions

- 5127 individual products / 866 vendors mentioned

Issues

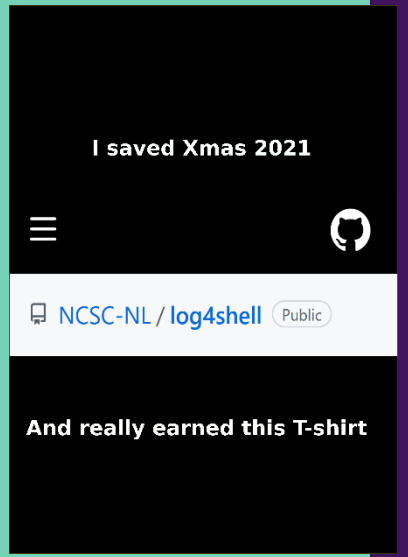
- Markdown table is difficult to keep in a valid format
- Preview of table in Github stops after 512KB of data in .md
- Organizing growing repo
- Validating loose format is time consuming
- Deciding when to end support

- 5127 individual products / 866 vendors mentioned

TLP:WHITE

International cooperation

- Initially resource heavy with two people updating the page, became much more manageable when we switched to pull requests
- BIG community effort, thank you all who contributed! Special thanks to CERT-EU and Cert-Bund
- Decision not to duplicate efforts and support one list was key. Where this was not possible we tried to synchronize.



Future

Github

- Will be used more often, when it is benefit to share operational information (Spring4Shell)
- Quick setup of Github actions to improve usability

Insight

- Structuring available information just as essential as providing new information

International

- Starting discussions on ways to contribute to incentives instead of duplicate


Questions?