MI-X Overview

The Challenge

EACH DAY, ORGANIZATIONS GRAPPLE WITH MANY CRITICAL VULNERABILITIES and scramble to understand if they are affected by that vulnerability before a threat actor figures it out first. Many times, their existing tools cannot help them make this determination. In order to do so, organizations need to:

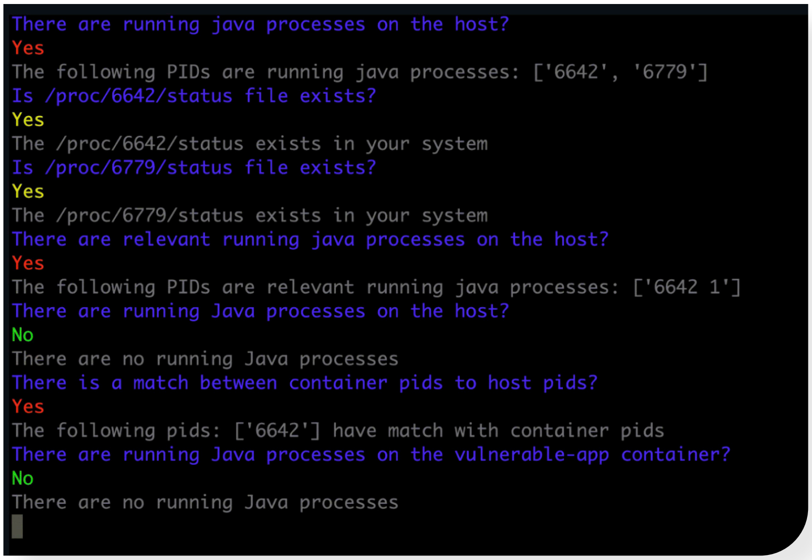
1. **Identify** the vulnerability in their environment
2. **Ascertain** whether that vulnerability is actually exploitable in order to have a mitigation/ remediation plan in place

What organizations need is a tool that can quickly address the two issues above. There are several challenges with current vulnerability scanners — they are not equipped to determine exploitability, take too long, and based on the nature of a specific vulnerability often miss it altogether — as was the case with the recently discovered Log4j vulnerability. The lack of proper tools gives threat actors a lot of time to exploit a flaw and do major damage.

What is MI-X

MI-X IS AN OPEN SOURCE CLI TOOL DEVELOPED BY REZILION'S vulnerability research that helps researchers and developers instantly find out if their containers and hosts are impacted by a specific vulnerability.

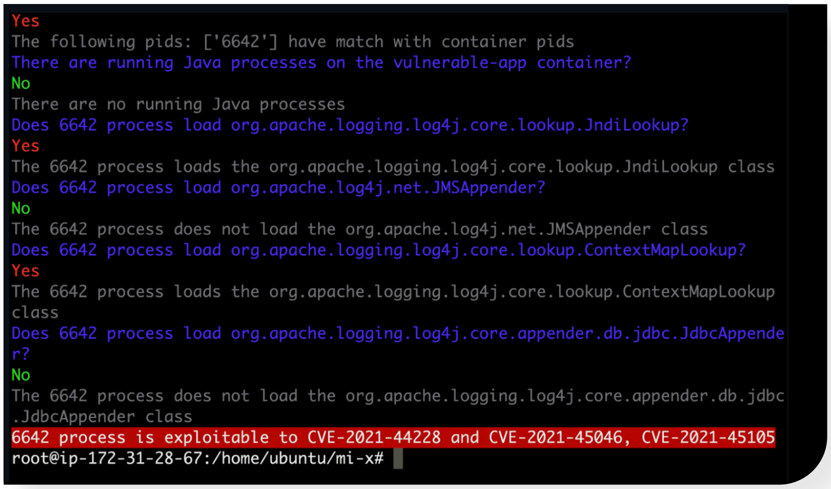
MI-X is ideal for researchers, developers, and small organizations to quickly detect the presence and exploitability of a known critical CVE so they can eliminate guesswork and focus on remediating immediately.



```
There are running java processes on the host?
Yes
The following PIDs are running java processes: ['6642', '6779']
Is /proc/6642/status file exists?
Yes
The /proc/6642/status exists in your system
Is /proc/6779/status file exists?
Yes
The /proc/6779/status exists in your system
There are relevant running java processes on the host?
Yes
The following PIDs are relevant running java processes: ['6642 1']
There are running Java processes on the host?
No
There are no running Java processes
There is a match between container pids to host pids?
Yes
The following pids: ['6642'] have match with container pids
There are running Java processes on the vulnerable-app container?
No
There are no running Java processes
```

MI-X is easily upgradeable to expand coverage of vulnerabilities. Security teams can quickly and strategically identify vulnerabilities, without the need for expensive tools. Through MI-X, users can:

- ✓ **Respond quickly to vulnerabilities:** With MI-X you can quickly identify and establish the exploitability of a known critical CVE.
- ✓ **Know why it's exploitable:** Don't just find the CVE but also get a detailed view of the criteria that need to be met for the vulnerability to be exploitable.
- ✓ **Plan your remediation:** Armed with the knowledge and context, users can act fast, shorten the attack window, and have an effective remediation plan.



```
Yes
The following pids: ['6642'] have match with container pids
There are running Java processes on the vulnerable-app container?
No
There are no running Java processes
Does 6642 process load org.apache.logging.log4j.core.lookup.JndiLookup?
Yes
The 6642 process loads the org.apache.logging.log4j.core.lookup.JndiLookup class
Does 6642 process load org.apache.log4j.net.JMSAppender?
No
The 6642 process does not load the org.apache.log4j.net.JMSAppender class
Does 6642 process load org.apache.logging.log4j.core.lookup.ContextMapLookup?
Yes
The 6642 process loads the org.apache.logging.log4j.core.lookup.ContextMapLookup
class
Does 6642 process load org.apache.logging.log4j.core.appender.db.jdbc.JdbcAppende
r?
No
The 6642 process does not load the org.apache.logging.log4j.core.appender.db.jdbc
.JdbcAppender class
6642 process is exploitable to CVE-2021-44228 and CVE-2021-45046, CVE-2021-45105
root@ip-172-31-28-67:/home/ubuntu/mi-x#
```

Key Features

- ✓ Quickly discover and identify if a specific vulnerability is present
- ✓ Know if the specific vulnerability is actually exploitable in your environment
- ✓ Understand the specific elements that make it exploitable
- ✓ Results are available as an output to the CLI or exported as a visual flowchart in PNG format.
- ✓ Over 20+ known vulnerabilities are supported
- ✓ Easily upgradeable to add coverage for a newly discovered vulnerability

How it Works

Available to download from the GitHub repository. MI-X is easy to set up and use.

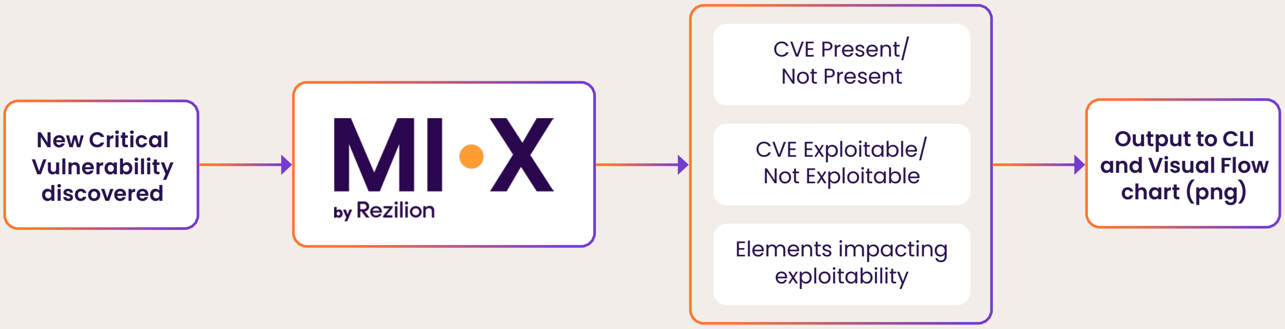
Step 1: Download MI-X on your host

Step 2: Execute MI-X on your host or on your running containers

Step 3: MI-X analyzes your host or running containers to identify the presence of a specific vulnerability in your environment

Step 4: Know if the identified vulnerability is exploitable and the justifications for exploitability

Step 5: Use the results to drive effective remediation


New Critical Vulnerability discovered
MI·X by Rezilion
CVE Present/ Not Present
CVE Exploitable/ Not Exploitable
Elements impacting exploitability
Output to CLI and Visual Flow chart (png)

Rezilion is a software attack surface management platform that helps enterprises detect, prioritize, and remediate software vulnerabilities. We have brought the same enterprise-class reliability and performance to MI-X, our open source tool is purpose-built to help researchers, developers, and small organizations quickly address any risk associated with urgent vulnerabilities. Download the tool here.

Get Started with Rezilion Solutions Learn more about Rezilion's software attack surface management platform at www.rezilion.com and get your 30-day free trial. Or see our platform in action and book a demo at https://www.rezilion.com/request-a-demo/.

About Rezilion

Rezilion's platform automatically secures the software you deliver to customers. Rezilion's continuous runtime analysis detects vulnerable software components on any layer of the software stack and determines their exploitability, filtering out up to 95% of identified vulnerabilities. Rezilion then automatically mitigates exploitable vulnerabilities across the SDLC, reducing vulnerability backlogs and remediation timelines from months to hours, while giving DevOps teams time back to build.

Learn more about Rezilion's software attack surface management platform at www.rezilion.com and get your 30-day free trial.