COMMUNITY
THE ASF CONFERENCE
CODE

Firsthand Analysis of Apache NiFi Vulnerability CVE-2023-34468

David Handermann, PMC Member of Apache NiFi, Software Engineer at Datavolo

Introduction – David Handermann

PMC Member
nifi.apache.org

Software Engineer
datavolo.io

Software Development Blog
exceptionfactory.com

Introduction

What is Apache NiFi **CVE-2023-34468**?

Potential Code Injection

with

Database Services Using H2

Introduction

CVE-2023-34468: Facts and Figures

- CVSS Base Score: **8.8**
- Reporter: **Matei Badanoiu** aka Mal Aware
- Resolution Author: **David Handermann**
- Affected Versions: Apache NiFi **0.0.2** to **1.21.0**
- Apache Jira Issue: **NIFI-11653**

Introduction

Vulnerability Review: **Disclosure to Reaction**

- Disclosure Timeline
- Impacted Components
- Resolution and Mitigating Factors
- Exploit Publication
- Security Reporting

Disclosure Timeline

Initial Disclosure on **2023-06-06**

- Reporter **emailed** Apache NiFi Security
- NiFi Security **acknowledged** reporting
- NiFi Security **created** Jira issue and CVE record
- NiFi Security **confirmed** finding
- Reporter **concurred** with CVE description

Disclosure Timeline

Initial Remediation on **2023-06-06**

- David Handermann **submitted** GitHub PR 7349
- Joe Witt **reviewed and merged** GitHub PR 7349
- Joe Witt **prepared** NiFi 1.22.0 Release Candidate 1
- Community began Release Candidate 1 **voting**

Disclosure Timeline

Remediation Released on **2023-06-12**

- Community **approved** NiFi 1.22.0 RC 1
- Joe Witt **released** Apache NiFi 1.22.0
- David Handermann **announced** CVE-2023-34468

Impacted Components

Database Drivers

provide

Code Execution

Impacted Components

Code Execution: **H2 Database Driver**

- H2 is relational database written in Java
- JDBC driver with no dependencies
- Open source under EPL 1.0 or MPL 2.0
- Runs with **JVM permissions**
- Supports **User-Defined Functions**

Impacted Components

Code Execution: **H2 Database Functions**

```
CREATE ALIAS RUNTIME_EXEC AS '
String execute(String command) {
  Runtime.getRuntime().exec(command);
  return "EXECUTED"
}

';
```

Impacted Components

Database Access: **Connection Pooling Services**

- Apache NiFi Database Connection Services
  - **DBCPConnectionPool**
  - **HikariCPConnectionPool**
- Configurable **Database Driver Location**
  - h2-2.1.214.jar in project work directory

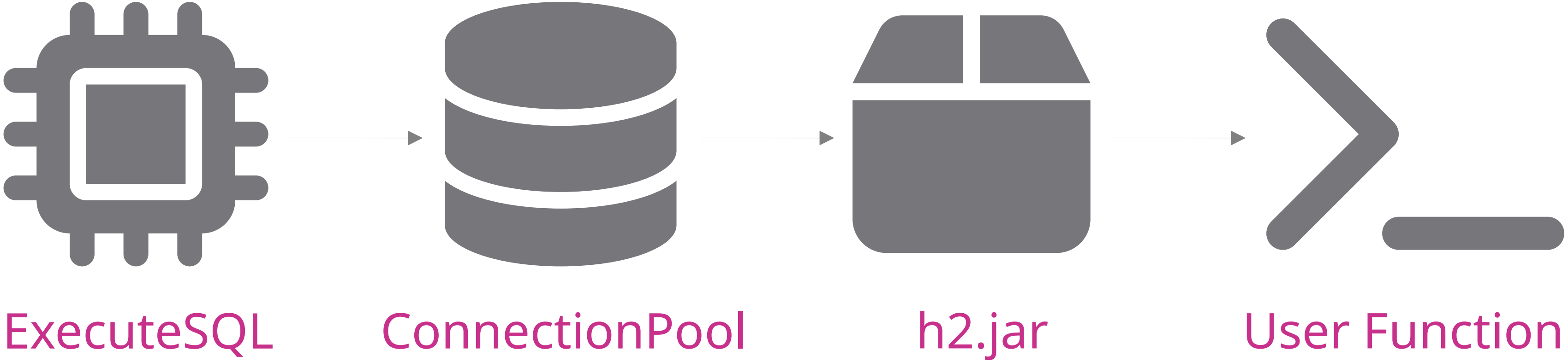
Impacted Components

Database Access: **SQL Processors**

- Apache NiFi Database Processors
  - **ExecuteSQL**
  - **PutSQL**
- Configurable **Connection Pooling Service**

Impacted Components

Database Access: **Vulnerable configuration**



ExecuteSQL → ConnectionPool → h2.jar → User Function

Resolution and Mitigating Factors

Disabling and **Deleting** Dangerous Defaults

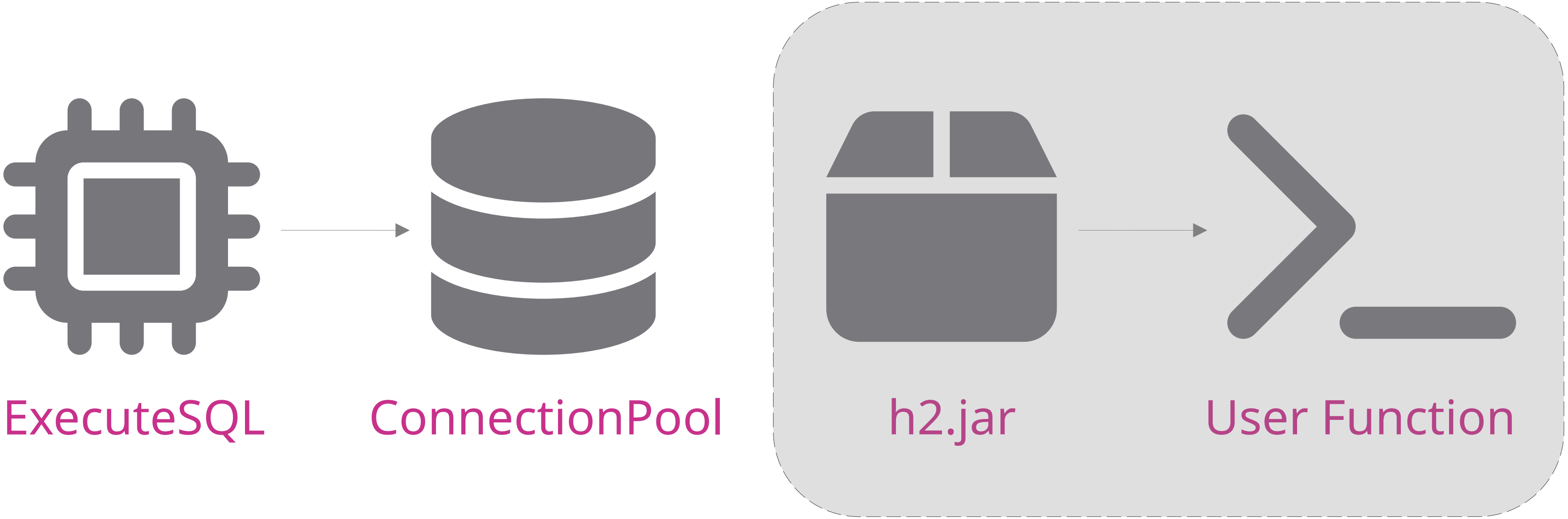
Resolution and Mitigating Factors

Initial Resolution: **Disabled H2 connections**

- NiFi 1.22.0 disabled connections with **jdbc:h2**
  - Connection Pool Services with URL Validation
- **Retained H2** for Flow Configuration History

Resolution and Mitigating Factors

Initial Resolution: **Blocked H2 connection pools**



Resolution and Mitigating Factors

Subsequent Issue: **CVE-2023-40037**

- Modified Connection URL could bypass validation
- Reported on **2023-08-03** Published on **2023-08-18**
- CVSS Base Score: **6.5**
- Reporter: Matei Badanoiu
- Affected Versions: Apache NiFi **1.21.0** to **1.23.0**

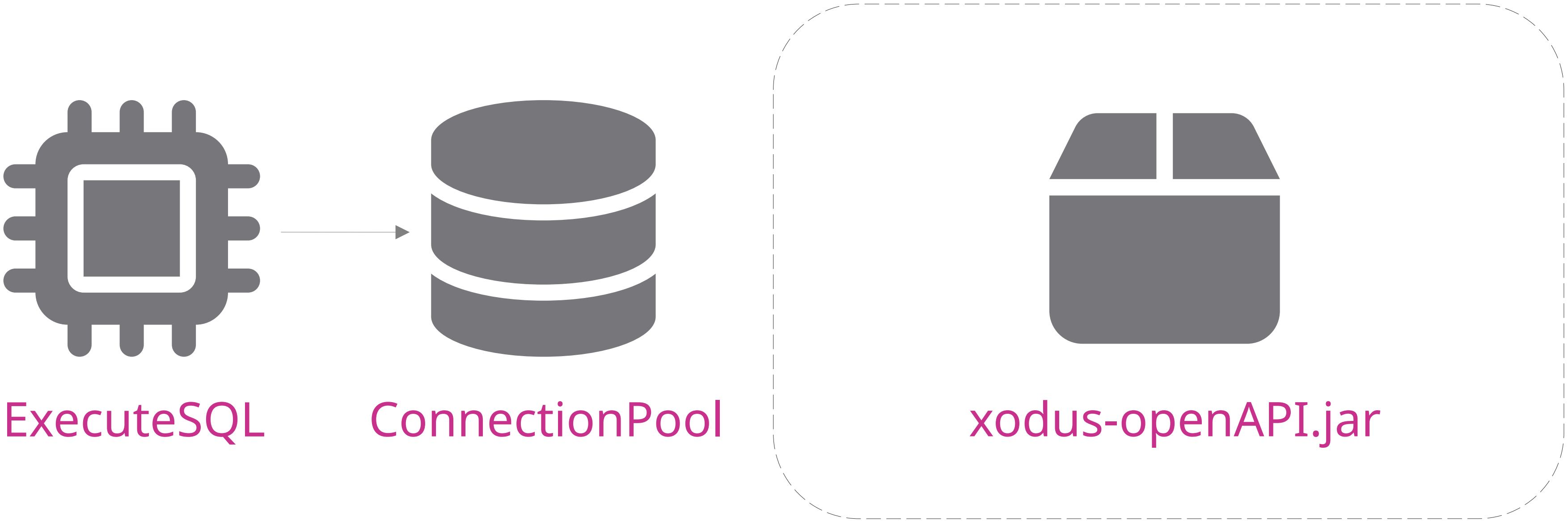
Resolution and Mitigating Factors

Additional Changes: **Removed H2 dependency**

- NiFi **1.24.0** removed H2 dependency
  - Flow Configuration History migration
- Replaced H2 with **JetBrains Xodus**
  - Transactional schema-less embedded database
  - Open sourced under Apache License 2.0

Resolution and Mitigating Factors

Additional Changes: **Replaced H2 with Xodus**



ExecuteSQL

ConnectionPool

xodus-openAPI.jar

Resolution and Mitigating Factors

Mitigating Factors: **Authentication** required

- NiFi 1.14.0 and following require authentication
  - Defaults to **Single User** Authentcation
- Authentication required for **flow configuration**

Resolution and Mitigating Factors

Mitigating Factors: **Authorization** required

- NiFi 1.14.0 and following require **authorization**
  - Single User Authorizer for local developers
- **Managed Authorizer** for multiple tenants
  - **Write permissions** required
- CVSS Privileges Required: **High**

Exploit Publication

Reproducible

Exploits

Reproducibility: **Publication Details**

- **Metasploit** Module
- Source: **Packet Storm**
- Author: Matei Badanoiu
- Published: 2023-08-30

Exploit Publication

Reproducibility: **Authentication required**

- **Username** and **password** required
- **Configuration privileges** required
- **Docker** deployment required
  - Based on H2 library location

Security Reporting

Severity

is not always
what it seems

Public Analysis: **Initial Reporting**

- **CYFIRMA Research** published report on **2023-09-28**
  - Emphasized **remote code execution**
  - Focused on vulnerability severity scoring
  - Noted numbers of deployed NiFi systems
  - Overlooked **access requirements**

Public Analysis: **Summary Articles**

- **CYFIRMA** generated podcast on 2023-09-29
- **SecurityWeek** summary on 2023-09-29
- **Cyber Security News** summary on 2023-10-02
- **OODA Loop** summary on 2023-09-29

Public Analysis: **The Telephone Game**

- **Apache NiFi** published CVE-2023-34468
  - **Reporter** released Metasploit Module
    - **CYFIRMA** summarized Metasploit Module
      - **Others** summarized CYFIRMA analysis

Beyond Headlines: **Bug or Feature?**

- NiFi supports custom **scripted** Processors
  - Requires **execute code** permission
- Why publish CVE-2023-34468?
  - **Unsupported** code execution

Conclusion

Read **Beyond the Score**

Conclusion

Stay connected

exceptionfactory.com