waratek

Customer Alert 20200608

Security researchers publish details and PoC for new RCE deserialization vulnerability (CVE-2020-9484) in Apache Tomcat

Waratek customers are protected by default rule

Background

A new proof of concept exploit has been released on GitHub and is being used to attack Apache Tomcat servers in the wild. New technical details of the vulnerability and how the exploit works have been published by Red Timmy Security following a report from pdd security research on 12 April 2020 to the Apache Tomcat Security team about a critical Remote Code Execution deserialization vulnerability that affects Apache Tomcat.

Discussion

CVE-2020-9484 is a critical deserialization flaw in Apache Tomcat that can lead to Remote Code Execution.

It is important to note that this vulnerability manifests only when the following conditions are met:

- The attacker can take control of the contents and filename on the server.
- The PersistenceManager is enabled and configured with a FileStore.
- The PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter.
- The attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over.
- There are known or unknown gadgets in the classpath that can be used to construct a gadget-chain to perform a Java deserialization attack

Default Tomcat configurations are not affected. To be affected the following needs to be configured in server.xml

```
    <Manager
className="org.apache.catalina.session.PersistentManager">
```

```
        <Store className="org.apache.catalina.session.FileStore"
directory="DIRECTORY"/>
    </Manager>
```

If these conditions are met then an attacker could trigger a remote code execution via deserialization by sending a specially-crafted HTTP request with a JSESSIONID cookie.

Using maliciously-crafted serialized gadget chains, attackers can execute arbitrary code (Remote Code Execution – RCE) in the context of the affected application. Successful attacks can allow attackers to completely compromise the system, including deploying ransomware. Failed attacks could also result in Denial-of-Service conditions. The vulnerability ranks 7.0 out of 10 on the CVSSv3 scale.

According to the fix from the Apache team, the flaw is located in the FileStore class which is missing proper input validation of the path of the deserialized file.

Products Affected

- Apache Tomcat 10.x < 10.0.0-M5
- Apache Tomcat 9.x < 9.0.35
- Apache Tomcat 8.x < 8.5.55
- Apache Tomcat 7.x < 7.0.104

Unaffected Versions

- Apache Tomcat 10.x >= 10.0.0-M5
- Apache Tomcat 9.x >= 9.0.35
- Apache Tomcat 8.x >= 8.5.55
- Apache Tomcat 7.x >= 7.0.104

References

- https://www.redtimmy.com/java-hacking/apache-tomcat-rce-by-deserialization-cve-2020-9484-write-up-and-exploit/
- https://nvd.nist.gov/vuln/detail/CVE-2020-9484
- https://github.com/masahiro331/CVE-2020-9484

Action Steps

Waratek Secure and *Waratek Upgrade* customers **are already protected** by the deserial/marshal rule that is standard protection in the Waratek application security platform. Waratek's process forking rule, available in *Waratek Patch, Secure* and *Upgrade* also mitigates the attacks. Waratek Secure rules provide protection against **known and zero-day attacks** with zero configuration and no source code changes.

Waratek's out-of-the-box zero-day protection not only protects the Apache Tomcat versions that are patched by the newer versions but also protects legacy, end-of-life Tomcat releases.

Non-Waratek customers are advised to:

1. Upgrade to the latest, patched Tomcat version as soon as possible
2. Monitor their Apache Tomcat logs for HTTP 500 errors that could indicate successful attacks.
3. Configure the sessionAttributeValueClassNameFilter with a regular expression that is suitable for the environment
4. Configure the JEP-290 global serialization blacklist with known, dangerous, gadgets

For more information about how Waratek provides zero-day protection against deserialization attacks and specifically against CVE-2020-9484 without downtime, source code or configuration changes, regular expressions or blacklists, please contact your Waratek representative or schedule a demonstration.

About Waratek

Some of the world's leading companies use Waratek's ARMR Security Platform to patch, secure and upgrade their mission critical applications. A pioneer in the next generation of application security solutions, Waratek makes it easy for security teams to instantly detect and remediate known vulnerabilities with no downtime, protect their applications from known and Zero Day attacks, and virtually upgrade out-of-support Java applications – all without time consuming and expensive source code changes or unacceptable performance overhead.

Waratek is the Cybersecurity Breakthrough Award's 2019 Overall Web Security Solution of the Year, is a previous winner of the RSA Innovation Sandbox Award, and more than a dozen other awards and recognitions. For more information, visit www.waratek.com.