ADOPTIUM

ECLIPSE FOUNDATION

Eclipse Temurin™

Trail of Bits

Security Assessment Response

June 17th, 2024

Follow-up to the Trail of Bits security assessment report published June 14th, 2024

Background

The Adoptium™ project produces high quality Java runtimes for use in mission-critical environments. The principal product of the Adoptium project is the Eclipse Temurin™ runtime available from https://adoptium.net. The Temurin runtime has been installed in many millions of enterprises and development environments to date, and continues to be actively developed and supported.

It is important to the Adoptium project and our users that the software we deliver is both safe and secure. The project is committed to a culture of continuous improvement through our secure development and supply-chain management procedures. To that end, the Eclipse Foundation received funding to actively support the Adoptium project in undertaking a security assessment to identify areas for further improvement.

The Eclipse Foundation engaged the Open Source Technology Improvement Fund as an independent audit company to oversee a review of the Temurin project, and specifically instructed the cybersecurity research and consulting firm Trail of Bits to conduct a detailed technical assessment of project areas where we considered such a review would be most valuable.

A full report on the Temurin security assessment is available publicly via OSTIF.org and on the Trail of Bits Publications Page. Readers are encouraged to first read the final report available at https://ostif.org/wp-content/uploads/2024/06/Temurin-Final-Report.pdf . This document describes the Adoptium project's response to that report. Readers should note that the assessment is a point in time piece of work, and that while the Trail of Bits team worked closely with the project members to understand and evaluate the technical details of Temurin, the project recognises that it is impossible to capture every possible security scenario or issue that may arise, and Adoptium remains responsible for the secure delivery of Temurin products.

Acknowledgements and Thanks

The Adoptium team is grateful to the Trail of Bits team for conducting a thorough assessment, and publishing a comprehensive report. We were able to work closely with the Trail of Bits team throughout the assessment to describe Temurin's architecture, answer technical

questions about the code, and provide assurances of the processes followed. It was a professional and productive engagement.

Thanks also go to the OpenSSF's Alpha-Omega project that provided funding to help Adoptium and other Eclipse Foundation projects improve their security, the Foundation itself for providing this opportunity to Adoptium, and the Adoptium project members that worked on achieving the resolutions.

Eclipse Temurin Secure Development

The Adoptium project follows a number of secure development practices that are designed to reduce vulnerabilities associated with software development and distribution. Many of these areas were also part of the security audit themes.

- **Provenance and Trusted Sources** : Adoptium builds source code from trusted source repositories, and takes dependencies and tools from trusted locations.

- **Version Control and Tagging** : All the code maintained by Adoptium projects is held in version controlled repositories administered by the Eclipse Foundation.

- **Infrastructure as Code** : To ensure that our infrastructure is securely managed and externally scrutinised we define and provision machines using the principles of Infrastructure as Code (IaC).

- **Reproducible Builds** : An important part of Adoptium's secure engineering practice is for community members to be able to verify the builds we produce through reproducibility.

- **Testing and Code-signing** : Adoptium validates and verifies the Eclipse Temurin releases using an extensive suite of software tests, and digitally signs all releases.

- **Audits and Verification** : All aspects of an Adoptium release are conducted in the open (except TCK proprietary compatibility testing), with regular reviews and validation of activity by a diverse set of participants.

Adoptium also follows the secure Supply chain Levels for Software Artifacts (SLSA) framework that helps to provide confidence that a set of inputs such as source code, libraries, and software packages, lead to a set of well-defined outputs such as a binary and software bill of materials. Temurin has achieved the highest Build track Level 3 accreditation for most platforms.

The supply chain management approach is further described in an Eclipse Foundation Case Study available at https://outreach.eclipse.foundation/adoptium-temurin-supply-chain-security

The Adoptium project uses third-party tools to monitor our infrastructure, including resource management tools, and unified detection and response / security information and event management tools in addition to multiple code scanners and analysers. The security and integrity of the code and our systems is continually monitored and audited within the project.

The project team determined that the most valuable engagement with Trail of Bits would cover the Adoptium infrastructure code (Ansible playbooks, Jenkins configuration, system management, etc.), product build scripts (used to create the Temurin product), and our Adoptium API implementation (used to distribute the product). These form critical parts of the project.

Detailed Response

The Trail of Bits security assessment resulted in a comprehensive report covering all areas requested by the project. The outcome of the assessment included concrete actionable items that the project could undertake to improve the security posture of the infrastructure, build, and distribution environment.

Details of the areas for improvement were provided to the project by Trail of Bits ahead of publication, giving us time to assess, review, and resolve each issue before they were made public.

The Adoptium team have corroborated the findings of the Trail of Bits team, determined a project-view of the resolution priority (in addition to the Trail of Bits severity assessment), and provided a response.

Resolutions

The following table outlines the actions taken as a result of each issue raised by the Trail of Bits assessment.

- **ToB Identifier**: The Trail of Bits team use unique identifiers for each issue raised, in the format “TOB-TEMURIN-<n>”, and we have used the same identifiers in this document when describing our responses.

- **ToB Severity** : Trail of Bits’ view of the severity of the issue identified. These are one of ‘Informational’, ‘Undetermined’, ‘Low’, ‘Medium’, or ‘High’ as defined in the Trail of Bits report.

- **ToB Summary** : A short description of the issue. Further details and a full description are in the Trail of Bits report.

- **Project Response** : A short description of how the issue was resolved by the Adoptium team. Each issue may be resolved by some number of code or process changes tracked in the Adoptium organisation’s GitHub repositories.

ToB Identifier	ToB Severity	ToB Summary	Project Response
TOB-TEMURIN-1	High	Command injection in WinRMscript	Mitigated by use of access control. Access has been restricted to the infrastructure team only. This issue is identified in a script used to test Adoptium’s infrastructure internally, and is not part of Temurin’s build or distribution processes. The job that runs this script has extremely controlled access, and anybody with permissions to exploit this already has direct machine access when required.

TOB-TEMURIN-3	High	Insecure installation of Xcode software	Resolved. Download secured with the use of checksum validation and major version check.
TOB-TEMURIN-4	High	Insecure software download in Ansible playbooks	Resolved. All identified insecure downloads secured using appropriate methods (switch to https downloads & checksum validations). Implementation of enhanced code scanning to check future changes do not cause a regression.
TOB-TEMURIN-5	High	Signature verification disabled during software installation	SLES12 & RHEL issues fixed. OpenSuse12 is EOL, and has been removed. This will be reworked to use OpenSuse LEAP to avoid the issue.
TOB-TEMURIN-7	High	Hostname verification disabled on MongoDB client	Resolved. Code updated to no longer require that hostname verification be disabled. DISABLE_MONGO_HOST_CHECK is never set to true in production.
TOB-TEMURIN-9	High	Insecure download using wget command	Resolved: Downloads now updated to use secure methods.
TOB-TEMURIN-13	High	SSH client disables host key verification	Insecure connection methods replaced in both Jenkins & Nagios. Some additional work is required to automate the adding of ssh keys to Nagios. These locations are considered benign because they are connecting to internal, short-lived, or local-only services.
TOB-TEMURIN-17	High	Code injection vulnerability in build-scripts pipeline jobs	Resolved, by access control methods. Access is restricted to those who can initiate build jobs.
TOB-TEMURIN-15	Medium	Use of unpinned third party workflow	Resolved. Remaining GitHub actions now use pinned versions / sha checksums everywhere.
TOB-TEMURIN-2	Low	Docker compose ports exposed on all interfaces	Resolved. Code updated and restricted to only expose required ports.
TOB-TEMURIN-6	Low	Missing integrity check in Dragonwell Dockerfile	Resolved. Unused by Adoptium, but code changes made to include integrity checks.

TOB-TEMURIN-8	Low	Red Hat Enterprise Linux image includes password	Resolved. The password is no longer included in the image. It has been moved to a build secret.
TOB-TEMURIN-12	Low	Missing integrity/auth check in jcov script download	Some artefact validation in place. Further work is planned to improve artefact handling to include storing a local secure hash value.
TOB-TEMURIN-10	Info	Hardcoded CA bundle password	Informational finding. This is standard Java practice. No action taken. The hardcoded password in this code is only used to allow the update/deployment of a new cacerts file, and is not used or available outside of these processes.
TOB-TEMURIN-11	Info	Hardcoded Vagrant VM password	Resolved by access control methods. Access has been restricted to the infrastructure team only. The job that runs this script has extremely controlled access, and anybody with permissions to exploit this already has direct machine access when required.
TOB-TEMURIN-14	Info	Compiler mitigations are not enabled	Informational finding. Work is in progress to determine which compiler flag changes could potentially be implemented when building a JDK while maintaining compatibility.
TOB-TEMURIN-16	Info	Third party deps used without signature/checksum	Resolved. Downloads are now secured, although none of these are used in the production of Temurin binaries.
TOB-TEMURIN-18	Info	Docker commands specify root user in containers	Informational finding. The scripts used in the issue are not used in production of the Temurin JDK binary deliverables, and are provided as part of a development toolset.
TOB-TEMURIN-19	Undetermined	Incorrect Dependabot configuration filename	Resolved. Dependabot action now working normally.

Further Work

The Trail of Bits report identified two areas that require action based upon their codebase maturity evaluation and security reviews.

1. Remediate the findings disclosed in their report.
2. Create a centralized list of all the code locations where Temurin adds external dependencies.

The findings have been addressed as described in the previous section. These have been resolved either through direct remediation, by refactoring the area of code identified, or by deep analysis of the actual usage of the identified area and assurance that the issue does not affect Temurin security.

It remains an open requirement to list locations where external dependencies are managed. This requires a period of design since Adoptium uses managed dependencies throughout the Temurin build and distribution process, whether directly or through implied dependencies - including the compilers, docker images, and underlying operating systems. We currently do not maintain a list of locations where they are managed, however, Temurin releases do include a full Software Bill of Materials (SBOM) covering all the dependencies of the runtime, and all the dependencies used during the build processes. Temurin can be rebuilt from the dependencies listed in the SBOM.

Adoptium have implemented the Trail of Bits recommendation to implement Semgrep application security checks throughout the project, utilising the rules developed during the security review.