Security Reports

HANDY HINT

Shiro v1 version notice

As of February 28, 2024, Shiro v1 was superseded by v2.

Table of Contents

Reporting a vulnerability

We strongly encourage people to report security vulnerabilities privately to our security list before disclosing them in a public forum.

Please note that the e-mail address below should only be used for reporting undisclosed security vulnerabilities in Apache Shiro and managing the process of fixing such vulnerabilities. We cannot accept regular bug reports or other queries at this address.

security@shiro.apache.org (mailto:security@shiro.apache.org)

Vulnerability Handling Process

An overview of the vulnerability handling process is:

- The reporter reports the vulnerability privately to security@shiro.apache.org (mailto:security@shiro.apache.org).
- The Apache Shiro PMC team works privately with the reporter to resolve the vulnerability.
- A new release of the Apache Shiro concerned is made that includes the fix.
- The vulnerability is publicly announced.

A more detailed description of the process (https://www.apache.org/security/committers.html) has been written for committers. Reporters of security vulnerabilities may also find it useful.

Apache Shiro Vulnerability Reports

CVE-2026-48589 (https://www.cve.org/CVERecord?id=CVE-2026-48589)

Apache Shiro’s Jakarta EE module used the HTTP Referer header in certain cases to issue redirect after a user login. In affected versions, insufficient validation of this client-controlled value could allow an attacker to influence the redirect target in applications using the Jakarta EE module. This issue affects Apache Shiro from 2.0-alpha to 2.2.0, and 3.0.0-alpha-1, only when using shiro-jakarta-ee integration module.

Mitigation: Upgrade to version 2.2.1, or 3.0.0-alpha-2 or later, which fixes the issue by validating the Referer header and restricting redirects only to relative paths within the current application context.

Credit: Apache Shiro would like to thank **Bartlomiej Dmitruk** for reporting this issue.

CVE-2026-44598 (https://www.cve.org/CVERecord?id=CVE-2026-44598)

With valid login credentials, URL Redirection to Untrusted Site ('Open Redirect'), Server-Side Request Forgery (SSRF) vulnerability in Apache Shiro. After successful login, Jakarta EE integration module uses shiroSavedRequest cookie to redirect to a particular web page after login. This cookie was not validated, and can be forged to send an HTTP GET request from the server itself to an arbitrary URL from the cookie. This issue affects Apache Shiro from 2.0-alpha to 2.1.0, and 3.0.0-alpha-1, only when using shiro-jakarta-ee integration module.

Mitigation: Upgrade to version 2.2.0, or 3.0.0-alpha-2 or later, which fixes the issue by encrypting the cookie.

Credit: Apache Shiro would like to thank **James Love** for reporting this issue.

CVE-2026-43827 (https://www.cve.org/CVERecord?id=CVE-2026-43827)

Default configurations of Apache Shiro have a session fixation vulnerability. This issue affects Apache Shiro from 1.0 to 2.1.0, and 3.0.0-alpha-1. In the affected versions, when a session already exists, it is not invalidated upon successful login, nor is a new session being generated with a new ID.

Mitigation: Upgrade to version 2.2.0, 3.0.0-alpha-2 or later, which fixes the issue by invalidating the existing session and creating a new session with a new ID upon successful login.

Credit: Apache Shiro would like to thank **Rasmus Moorats** for reporting this issue.

CVE-2026-43828 (https://www.cve.org/CVERecord?id=CVE-2026-43828)

Default configurations of Apache Shiro send sensitive cookies in HTTPS session without 'Secure' attribute. This issue affects Apache Shiro from 1.0 to 2.1.0, and 3.0.0-alpha-1. In the affected versions, Shiro-native session manager, as well as Remember-Me manager sends JSESSIONID and rememberMe cookies without `secure` attribute by default.

Mitigation: Upgrade to version 2.2.0, 3.0.0-alpha-2 or later, which fixes the issue by setting the `secure` attribute.

Credit: Apache Shiro would like to thank **Meteor_Kai** for reporting this issue.

CVE-2026-23903 (https://www.cve.org/CVERecord?id=CVE-2026-23903)

If static files are served from a case-insensitive filesystem, such as default macOS setup, static files may be accessed by varying the case of the filename in the request. If only lower-case (common default) filters are present in Shiro, they may be bypassed this way. The issue only affects static files.

Shiro 2.1.0 and later has a new parameters to remediate this issue shiro.ini: `filterChainResolver.caseInsensitive = true` application.properties: `shiro.caseInsensitive=true`

Shiro 3.0.0 and later (upcoming) makes this the default.

Mitigation: Upgrade to version 2.1.0 or later, which fixes the issue.

Credit: Apache Shiro would like to thank **Jesse Yang** for reporting this issue.

CVE-2026-23901 (https://www.cve.org/CVERecord?id=CVE-2026-23901)

Prior to Shiro 2.1.0, code paths for non-existent vs. existing users are different enough, that a brute-force attack may be able to tell, by timing the requests only, determine if the request failed because of a non-existent user vs. wrong password.

The most likely attack vector is a local attack only.

Mitigation: Upgrade to version 2.1.0 or later, which fixes the issue, or ensure that the infrastructure-level mitigations are in place to prevent brute-force attacks, such as rate-limiting or account lockout.

Credit: Apache Shiro would like to thank **4ra1n** and **Y4tacker** for reporting this issue.

CVE-2023-46749 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46749)

Apache Shiro before 1.13.0 or 2.0.0-alpha-4, may be susceptible to a path traversal attack that results in an authentication bypass when used together with path rewriting

Mitigation: Update to Apache Shiro 1.13.0+ or 2.0.0-alpha-4+, or ensure `blockSemicolon` is enabled (this is the default).

CVE-2023-46750 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46750)

URL Redirection to Untrusted Site ('Open Redirect') vulnerability when "form" authentication is used in Apache Shiro.

Mitigation: Update to Apache Shiro 1.13.0+ or 2.0.0-alpha-4+.

CVE-2023-34478 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34478)

Apache Shiro, before 1.12.0 or 2.0.0-alpha-3, may be susceptible to a path traversal attack that results in an authentication bypass when used together with APIs or other web frameworks that route requests based on non-normalized requests.

Mitigation: Update to Apache Shiro 1.12.0+ or 2.0.0-alpha-3+.

Credit: Apache Shiro would like to thank **swifty tk** for reporting this issue.

CVE-2023-22602 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22602)

When using Apache Shiro before 1.11.0 together with Spring Boot 2.6+, a specially crafted HTTP request may cause an authentication bypass. The authentication bypass occurs when Shiro and Spring Boot are using different pattern-matching techniques. Both Shiro and Spring Boot < 2.6 default to Ant style pattern matching.

Mitigation: Update to Apache Shiro 1.11.0, or set the following Spring Boot configuration value:

```
spring.mvc.pathmatch.matching-strategy = ant_path_matcher
```

Credit: Apache Shiro would like to thank v3ged0ge and Adamytd for reporting this issue.

CVE-2022-40664 (https://cve.mitre.org/cgi-bin/cvename.cgi?

name=CVE-2022-40664)

Apache Shiro before 1.10.0, Authentication Bypass Vulnerability in Shiro when forwarding or including via RequestDispatcher.

CVE-2022-32532 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32532)

Apache Shiro before 1.9.1, A RegexRequestMatcher can be misconfigured to be bypassed on some servlet containers. Applications using RegExPatternMatcher with `.` in the regular expression are possibly vulnerable to an authorization bypass.

CVE-2021-41303 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41303)

Apache Shiro before 1.8.0, when using Apache Shiro with Spring Boot, a specially crafted HTTP request may cause an authentication bypass.

CVE-2020-17523 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17523)

Apache Shiro before 1.7.1, when using Apache Shiro with Spring, a specially crafted HTTP request may cause an authentication bypass.

CVE-2020-17510 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17510)

Apache Shiro before 1.7.0, when using Apache Shiro with Spring, a specially crafted HTTP request may cause an authentication bypass.

If you are NOT using Shiro's Spring Boot Starter (`shiro-spring-boot-web-starter`), you must configure add the `ShiroRequestMappingConfig` autoconfiguration to your application (/spring-framework.html#web_applications) or configure the equivalent manually (https://github.com/apache/shiro/blob/shiro-root-1.7.0/support/spring/src/main/java/org/apache/shiro/spring/web/config/ShiroRequestMappingConfig.java#L28-L30).

CVE-2020-13933 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13933)

Apache Shiro before 1.6.0, when using Apache Shiro, a specially crafted HTTP request may cause an authentication bypass.

CVE-2020-11989 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11989)

Apache Shiro before 1.5.3, when using Apache Shiro with Spring dynamic controllers, a specially crafted request may cause an authentication bypass.

CVE-2020-1957 (https://cve.mitre.org/cgi-bin/cvename.cgi?

name=CVE-2020-1957)

Apache Shiro before 1.5.2, when using Apache Shiro with Spring dynamic controllers, a specially crafted request may cause an authentication bypass.

CVE-2019-12422 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12422)

Apache Shiro before 1.4.2, when using the default "remember me" configuration, cookies could be susceptible to a padding attack.

CVE-2016-6802 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6802)

Apache Shiro before 1.3.2 allows attackers to bypass intended servlet filters and gain access by leveraging use of a non-root servlet context path.

CVE-2016-4437 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4437)

Apache Shiro before 1.2.5, when a cipher key has not been configured for the "remember me" feature, allows remote attackers to execute arbitrary code or bypass intended access restrictions via an unspecified request parameter.

CVE-2014-0074 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0074)

Apache Shiro 1.x before 1.2.3, when using an LDAP server with unauthenticated bind enabled, allows remote attackers to bypass authentication via an empty (1) username or (2) password.

CVE-2010-3863 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3863)

Apache Shiro before 1.1.0, and JSecurity 0.9.x, does not canonicalize URI paths before comparing them to entries in the shiro.ini file, which allows remote attackers to bypass intended access restrictions via a crafted request, as demonstrated by the /./account/index.jsp URI.

Edit this page on GitHub (https://github.com/apache/shiro-site/edit/main/src/site/content/security-reports.adoc)