Improper Certificate Validation in verifier

Moderate **Hayden-IO** published **GHSA-xm5m-wgh2-rrg3** yesterday

Package

github.com/sigstore/timestamp-authority/v2/pkg/verification (Go)

Affected versions	Patched versions
<= 2.0.5	2.0.6

Description

Authorization bypass via certificate bag manipulation in sigstore/timestamp-authority verifier

An authorization bypass vulnerability exists in sigstore/timestamp-authority verifier (timestamp-authority/v2/pkg/verification): `VerifyTimestampResponse` function correctly verifies the certificate chain but when the TSA specific constraints are verified in `VerifyLeafCert`, the first non-CA certificate from the PKCS#7 certificate bag is used instead of the leaf certificate from the certificate chain. An attacker can exploit this by prepending a forged certificate to the certificate bag while the message is signed with an authorized key. The library validates the signature using the one certificate but performs authorization checks on the another, allowing an attacker to bypass some authorization controls.

This vulnerability does **not** apply to timestamp-authority service, only to users of `timestamp-authority/v2/pkg/verification` package.

This vulnerability does **not** apply to sigstore-go even though it is a user of `timestamp-authority/v2/pkg/verification`: Providing `TSACertificate` option to `VerifyTimestampResponse` fully mitigates the issue.

Patches

The issue will be fixed in timestamp-authority 2.0.6

Workarounds

Users of `VerifyTimestampResponse` can use the `TSACertificate` option to specify the exact certificate they expect to be used: this fully mitigates the issue.

References

This issue was found after reading CVE-2026-33753 / GHSA-3xxc-pwj6-jgrj (originally reported by **@Jaynornj** and **@Pr00fOf3xpl0it**)

Severity

Moderate 5.5 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	None

Learn more about base metrics

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

CVE ID

CVE-2026-39984

Weaknesses

▶ CWE-295

Credits

jku Finder