EEF-CVE-2026-32144

See a problem?
Please try reporting it to the source first.

Source	https://cna.erlef.org/osv/EEF-CVE-2026-32144.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-32144.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-32144
Aliases	CVE-2026-32144 GHSA-gxrm-pf64-99xm
Published	2026-04-07T12:28:00.767Z
Modified	2026-04-07T15:00:15.346311Z
Severity	7.6 (High) CVSS_V4 - CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:L/SI:L/SA:N CVSS Calculator
Summary	OCSP designated-responder authorization bypass via missing signature verification

Details

Summary

Improper Certificate Validation vulnerability in Erlang OTP public*key (pubkey*ocsp module) allows OCSP designated-responder authorization bypass via missing signature verification.

The OCSP response validation in public*key:pkix*ocsp_validate/5 does not verify that a CA-designated responder certificate was cryptographically signed by the issuing CA. Instead, it only checks that the responder certificate's issuer name matches the CA's subject name and that the certificate has the OCSPSigning extended key usage. An attacker who can intercept or control OCSP responses can create a self-signed certificate with a matching issuer name and the OCSPSigning EKU, and use it to forge OCSP responses that mark revoked certificates as valid.

This affects SSL/TLS clients using OCSP stapling, which may accept connections to servers with revoked certificates, potentially transmitting

sensitive data to compromised servers. Applications using the public_key:pkix_ocsp_validate/5 API directly are also affected, with impact depending on usage context.

This vulnerability is associated with program files lib/public_key/src/pubkey_ocsp.erl and program routines pubkey_ocsp:is_authorized_responder/3.

This issue affects OTP from OTP 27.0 until OTP 28.4.2 and 27.3.4.10 corresponding to public_key from 1.16 until 1.20.3 and 1.17.1.2, and ssl from 11.2 until 11.5.4 and 11.2.12.7.

Workaround

For SSL users:

- Do not enable OCSP validation setting (current default is {stapling, no_staple})
- Use CRL-based revocation checking by setting the {crl_check, true} SSL option instead

For applications using public_key:pkix_ocsp_validate/5 directly:

- Pass {is_trusted_responder_fun, Fun} option with a function that validates trusted responder certificates
- Restrict OCSP responder access to trusted endpoints via network controls (only applicable if you control the OCSP infrastructure)

Configuration

SSL/TLS must be configured with OCSP stapling enabled (e.g., {stapling, staple}), or the application must call public_key:pkix_ocsp_validate/5 directly. OCSP stapling is disabled by default ({stapling, no_staple}).

Database specific


```
{
    "cpe_ids": [
        "cpe:2.3:a:erlang:erlang\\/otp:*:*:*:*:*:*:*:*"
    ],
    "capec_ids": [
        "CAPEC-459"
    ],
    "cwe_ids": [
        "CWE-295"
    ]
}
```


References

https://github.com/erlang/otp/security/advisories/GHSA-gxrm-pf64-99xm

https://cna.erlef.org/cves/CVE-2026-32144.html

https://www.erlang.org/doc/system/versions.html#order-of-versions

https://github.com/erlang/otp/commit/ac7ff528be857c5d35eb29c7f24106e3a16d4891

https://github.com/erlang/otp/commit/49033a6d93a5be0ee0dce04e1fb8b4ae7de1e0c0

Credits

Igor Morgenstern / Aisle Research - REPORTER

Jakub Witczak - REMEDIATION_DEVELOPER

Ingela Anderton Andin - REMEDIATION_REVIEWER

Affected packages

Git
github.com/erlang/otp

Affected ranges

Type GIT

Repo https://github.com/erlang/otp

Events Introduced
601a012837ea0a5c8095bf24223132824177124d
Fixed
ac7ff528be857c5d35eb29c7f24106e3a16d4891
Fixed
49033a6d93a5be0ee0dce04e1fb8b4ae7de1e0c0

Affected versions

- OTP-27.*
- OTP-28.*
- OTP-29.*
- Other

Database specific

▸ source