OCSP designated-responder authorization bypass — missing signature verification (RFC 6960 §4.2.2.2)

High **u3s** published **GHSA-gxrm-pf64-99xm** 2 weeks ago

Package

OTP

Affected versions	Patched versions
>= 27.0	27.3.4.10, 28.4.2

public_key (OTP)

>= 1.16	1.17.1.2, 1.20.3

ssl (OTP)

>= 11.2	11.2.12.7, 11.5.4

Description

Impact

For Erlang/OTP's internal usage (TLS client with OCSP stapling)

- Clients running TLS (SSL) may accept connections to servers with revoked certificates
- Clients may transmit sensitive data to compromised servers
- Requires attacker to control or MITM the server being validated
- Note: Erlang/OTP TLS (SSL) server does not support OCSP stapling
- Note: For legacy reasons the client was actually implemented and documented to do a best effort validation, which by default makes it unreliable. This is now addressed and a must staple behavior is enforced unless user implements its own fallback validation if the staple is missing.

For applications using public_key:pkix_ocsp_validate/5 API

- Impact depends on usage context
- Server-side client certificate validation: authentication bypass
- Other scenarios: variable impact

Workarounds

For TLS (SSL) users

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

For applications using `public_key:pkix_ocsp_validate/5` directly

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

Affected/Unaffected Versions

A version larger than or equal to one of the listed *patched versions* is **unaffected**; *otherwise*, a version that satisfies an expression listed under *affected versions* is **affected**, and if it does not, it is **unaffected**.

The documentation of the new *OTP version scheme* describes how versions should be compared. Note that versions used prior to OTP 17.0, when the new *OTP version scheme* was introduced, are never listed since it is not well defined how to compare those versions.

In the case of this vulnerability, versions prior to OTP 27.0 are unaffected.

Credits

Thanks to Igor Morgenstern at Aisle Research for finding and responsibly disclosing this vulnerability to the Erlang/OTP project.

Severity

High 7.6 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network

Attack Complexity	Low
Attack Requirements	Present
Privileges Required	None
User interaction	Passive
Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	None
Subsequent System Impact Metrics	
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-32144

Weaknesses

▶ CWE-295

Credits

imorgenstern	Reporter
IngelaAndin	Remediation reviewer