Crypt::PK key generation is not fork safe and will generate identical keys

Moderate **karel-m** published **GHSA-24c2-gp6c-24c6** 3 hours ago

Package

CryptX

Affected versions

<= 0.087

Patched versions

0.088

Description

Unlike the Crypt:PRNG modules, the PRNG used for generating keys for the Crypt::PK modules shares state and is not fork-safe is the object is created before forking.

A simple demonstration,

```
use feature 'say';

use Crypt::PK::RSA;

my $pk = Crypt::PK::RSA->new;

my $pid = fork() // die "failed to fork";

say "pid = $pid";

$pk->generate_key;

say $pk->export_key_jwk_thumbprint('SHA256');

waitpid($pid,0);
```

This will output two identical keys.

Note that use in preforking services (e.g. a web server running Starman) makes this issue occurring in production code likely.

Please invite **@stigtsp** from CPANSec (the finder) to contribute to this.

Severity

Moderate

CVE ID

CVE-2026-41564

Weaknesses

No CWEs

Credits

 **stigtsp** Finder