Memory leaks in code encrypting and verifying RSA payloads

High **gdams** published **GHSA-78hx-gp6g-7mj6** on Mar 20, 2024

Package

github.com/golang-fips/go (Go)

Affected versions	Patched versions
<= 1.22.1	None

github.com/golang-fips/openssl/openssl (Go)

<= 0	None

github.com/golang-fips/openssl/v2 (Go)

<= 2.0.0	2.0.1

github.com/microsoft/go (Go)

<= 1.22.1-1	1.22.1-2
<= 1.21.8-1	1.21.8-2

github.com/microsoft/go-crypto-openssl/openssl (Go)

<= 0.2.8	0.2.9

Description

Using crafted public RSA keys which are not compliant with SP 800-56B can cause a small memory leak when encrypting and verifying payloads.

An attacker can leverage this flaw to gradually erode available memory to the point where the host crashes for lack of resources. Upon restart the attacker would have to begin again, but nevertheless there is the potential to deny service.

Severity

High 7.5 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2024-1394

Weaknesses

No CWEs

Credits

 **qmuntal** Finder