

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: [Privacy Policy](#)



Manage Preferences

more [here](#) .

# CVE-2018-12437 PUBLISHED

[View JSO](#)

## Required CVE Record Information

### CNA: MITRE Corporation

**Updated:** 2020-07-28

**Published:** 2018-06-15 **Updated:** 2020-07-28

#### Description

LibTomCrypt through 1.18.1 allows a memory-cache side-channel attack on ECDSA signatures, aka the Return Of the Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.

#### Product Status

[Learn more](#)

*Information not provided*

#### References 2 Total

- <https://www.nccgroup.trust/us/our-research/technical-advisory-return-of-the-hidden-number-problem/>
- [security.gentoo.org: GLSA-202007-53](#) vendor-advisory

### CVE Program

#### References 2 Total

- <https://www.nccgroup.trust/us/our-research/technical-advisory-return-of-the-hidden-number-problem/>
- [security.gentoo.org: GLSA-202007-53](#) vendor-advisory x\_transferred

#### Policies & Cookies

- [Terms of Use](#)
- [Website Security Policy](#)

#### Media

- [News](#)
- [Blogs](#)

#### Social Media



#### Contact

- [CVE Program Support](#)
- [CNA Partners](#)

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: [Privacy Policy](#)

[Department of Homeland Security \(DHS\)](#) [Cybersecurity and Infrastructure Security Agency \(CISA\)](#). Copyright © 1999-2026, [The MITRE Corporation](#). CVE is a trademark and the CVE logo is a registered trademark of The MITRE Corporation.

Links that redirect to external websites [↗](#) will open a new window or tab depending on the web browser used.