

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

[Accept](#)

[Deny Non-Essential](#)

[Manage Preferences](#)

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. [Privacy Policy](#)