



# CVE-2021-24117

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-24117                                                                                                          |
| <b>State</b>           | PUBLIC                                                                                                                  |
| <b>Assigner</b>        | cve@mitre.org                                                                                                           |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                            |
| <b>Published</b>       | 2021-07-14 14:15:00 UTC                                                                                                 |
| <b>Updated</b>         | 2022-05-13 17:36:00 UTC                                                                                                 |
| <b>Description</b>     | In Apache Teaclave Rust SGX SDK 1.1.3, a side-channel vulnerability in base64 PEM file decoding allows system-level (ac |

## Risk And Classification

### Problem Types: CWE-203

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                           | Product                          | Version | Update | Edition | Language |
|-------------|----------------------------------|----------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Apache</a>           | <a href="#">Teaclave Sgx Sdk</a> | 1.1.3   | All    | All     | All      |
| Application | <a href="#">Sgx Tstd Project</a> | <a href="#">Sgx Tstd</a>         | 1.1.3   | All    | All     | All      |

## References

| Reference                                                                           | Source  | Link                         | Tags                |
|-------------------------------------------------------------------------------------|---------|------------------------------|---------------------|
| fix · dingelish/rust-base64@a554b7a · GitHub                                        | MISC    | <a href="#">github.com</a>   |                     |
| sgx_tstd 1.1.1 - Docs.rs                                                            | MISC    | <a href="#">docs.rs</a>      |                     |
| util-lookup/cve-vulnerability-publication.md at main · UzL-ITS/util-lookup · GitHub | MISC    | <a href="#">github.com</a>   |                     |
| CVE Program record                                                                  | CVE.ORG | <a href="#">www.cve.org</a>  | canonical           |
| NVD vulnerability detail                                                            | NVD     | <a href="#">nvd.nist.gov</a> | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)