



# CVE-2017-13095

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-13095                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | cert@cert.org                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2018-07-13 20:29:00 UTC                                                                                                     |
| <b>Updated</b>         | 2019-10-09 23:23:00 UTC                                                                                                     |
| <b>Description</b>     | The P1735 IEEE standard describes flawed methods for encrypting electronic-design intellectual property (IP), as well as th |

## Risk And Classification

**Problem Types:** CWE-310

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|---------|---------|--------|---------|----------|
| Operating System | -      | -       | -       | All    | All     | All      |
| Operating System | -      | -       | -       | All    | All     | All      |

## References

| Reference                                                                                         | Source  | Link                                                            |
|---------------------------------------------------------------------------------------------------|---------|-----------------------------------------------------------------|
| IEEE P1735 Multiple Cryptographic Local Security Weaknesses                                       | BID     | <a href="http://www.securityfocus.com">www.securityfocus.co</a> |
| Vulnerability Note VU#739007 - IEEE P1735 implementations may have weak cryptographic protections | CERT-VN | <a href="http://www.kb.cert.org">www.kb.cert.org</a>            |
| CVE Program record                                                                                | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                    |
| NVD vulnerability detail                                                                          | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                  |

No vendor comments have been submitted for this CVE.

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

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)