



# CVE-2021-21850

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-21850                                                                                                             |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | talos-cna@cisco.com                                                                                                        |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2021-08-25 19:15:00 UTC                                                                                                    |
| <b>Updated</b>         | 2022-05-31 19:00:00 UTC                                                                                                    |
| <b>Description</b>     | An exploitable integer overflow vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advan |

## Risk And Classification

### Problem Types: CWE-190

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                      | Version | Update | Edition | Language |
|------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 11.0    | All    | All     | All      |
| Application      | <a href="#">Gpac</a>   | <a href="#">Gpac</a>         | 1.0.1   | All    | All     | All      |

## References

| Reference                                                                             | Source  | Link                                                             | Tags          |
|---------------------------------------------------------------------------------------|---------|------------------------------------------------------------------|---------------|
| Debian -- Security Information -- DSA-4966-1 gpac                                     | DEBIAN  | <a href="http://www.debian.org">www.debian.org</a>               |               |
| TALOS-2021-1297    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence | MISC    | <a href="http://talosintelligence.com">talosintelligence.com</a> |               |
| CVE Program record                                                                    | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                     | canonical     |
| NVD vulnerability detail                                                              | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                   | canonical, ar |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[178779](#) Debian Security Update for gpac (DSA 4966-1)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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)