



# CVE-2021-40394

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

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-40394                                                                                                               |
| <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>       | 2021-12-22 19:15:00 UTC                                                                                                      |
| <b>Updated</b>         | 2023-09-30 17:15:00 UTC                                                                                                      |
| <b>Description</b>     | An out-of-bounds write vulnerability exists in the RS-274X aperture macro variables handling functionality of Gerbv 2.7.0 an |

## Risk And Classification

**Problem Types:** CWE-787

## 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> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 11.0    | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Application      | <a href="#">Gerbv Project</a> | <a href="#">Gerbv</a>        | 2.7.0   | All    | All     | All      |

## References

| Reference                                                                             | Source  | Link                                                              | Tags          |
|---------------------------------------------------------------------------------------|---------|-------------------------------------------------------------------|---------------|
| [SECURITY] [DLA 3593-1] gerbv security update                                         | MLIST   | <a href="https://lists.debian.org">lists.debian.org</a>           |               |
| Debian -- Security Information -- DSA-5306-1 gerbv                                    | DEBIAN  | <a href="https://www.debian.org">www.debian.org</a>               |               |
| TALOS-2021-1404    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence | MISC    | <a href="https://talosintelligence.com">talosintelligence.com</a> |               |
| CVE Program record                                                                    | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                     | canonical     |
| NVD vulnerability detail                                                              | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                   | canonical, ar |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[181448](#) Debian Security Update for gerbv (DSA 5306-1)

[183774](#) Debian Security Update for gerbv (CVE-2021-40394)

[6000041](#) Debian Security Update for gerbv (DLA 3593-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)