



# CVE-2021-38423

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

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-38423                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                       |
| <b>Assigner</b>        | ics-cert@hq.dhs.gov                                                                                                          |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2022-05-05 17:15:00 UTC                                                                                                      |
| <b>Updated</b>         | 2022-05-13 03:47:00 UTC                                                                                                      |
| <b>Description</b>     | All versions of GurumDDS improperly calculate the size to be used when allocating the buffer, which may result in a buffer o |

## Risk And Classification

**Problem Types:** CWE-131

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                | Product                  | Version | Update | Edition | Language |
|-------------|-----------------------|--------------------------|---------|--------|---------|----------|
| Application | <a href="#">Gurum</a> | <a href="#">Gurumdds</a> | All     | All    | All     | All      |

## References

| Reference                                                                  | Source  | Link                                           | Tags                |
|----------------------------------------------------------------------------|---------|------------------------------------------------|---------------------|
| Multiple Data Distribution Service (DDS) Implementations (Update A)   CISA | CONFIRM | <a href="http://www.cisa.gov">www.cisa.gov</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, analysis |

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Federico Maggi (Trend Micro Research), Ta-Lun Yen, and Chizuru Toyama (TXOne Networks, Trend Micro) reported these vulnerabilities to CISA. In addition, Patrick Kuo, Mars Cheng (TXOne Networks, Trend Micro), Víctor Mayoral-Vilches (Alias Robotics), and Erik Boasson (ADLINK Technology) also contributed to this research.

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

© [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](#)