



# CVE-2021-46462

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-46462  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2022-02-14 22:15:00 UTC   |
| <b>Updated</b>         | 2022-03-24 14:33:00 UTC   |
| <b>Description</b>     | njs through 0.7.1, used in NGINX, was discovered to contain a segmentation violation via njs_object_set_prototype in /src/r |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | F5     | Njs     | All     | All    | All     | All      |
| Application | Nginx  | Njs     | All     | All    | All     | All      |

## References

| Reference  | Source  | Link                                | Tags   |
|--|---------|-------------------------------------|--------|
| Fixed Function.prototype.apply() with slow arrays. · nginx/njs@39e8fa1 · GitHub                  | MISC    | <a href="#">github.com</a>          |        |
| SEGV /njs/src/njs_object.c:2136:24 in njs_object_set_prototype · Issue #449 · nginx/njs · GitHub | MISC    | <a href="#">github.com</a>          |        |
| February 2022 NGINX Vulnerabilities in NetApp Products   NetApp Product Security                 | CONFIRM | <a href="#">security.netapp.com</a> |        |
| CVE Program record   | CVE.ORG | <a href="#">www.cve.org</a>         | canoni |
| NVD vulnerability detail   | NVD     | <a href="#">nvd.nist.gov</a>        | canoni |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

502121 Alpine Linux Security Update for njs

502226 Alpine Linux Security Update for nginx

504100 Alpine Linux Security Update for nginx

[504190](#) Alpine Linux Security Update for nginx

[505091](#) Alpine Linux Security Update for njs

© [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](#).

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