



CVE-2021-21389

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-21389 |
| State | PUBLIC |
| Assigner | security-advisories@github.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-03-26 21:15:00 UTC |
| Updated | 2021-04-01 15:45:00 UTC |
| Description | BuddyPress is an open source WordPress plugin to build a community site. In releases of BuddyPress from 5.0.0 before 7.2.1, the REST API endpoint /wp-json/buddypress/v1/users/ is not properly sanitized, allowing an attacker to bypass authentication and access sensitive information. |

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------------------------|----------------------------|---------|--------|---------|----------|
| Application | Buddypress | Buddypress | All | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|---|-----------|
| Version 7.2.1 · BuddyPress Codex | MISC | codex.buddypress.org | |
| BuddyPress privilege escalation via REST API · Advisory · buddypress/BuddyPress · GitHub | CONFIRM | github.com | |
| BuddyPress 7.2.1 Security Release · BuddyPress.org | MISC | buddypress.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical |

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](#).

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