



CVE-2020-5244

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

Summary

CVE	CVE-2020-5244
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-24 18:15:00 UTC
Updated	2020-02-25 21:34:00 UTC
Description	In BuddyPress before 5.1.2, requests to a certain REST API endpoint can result in private user data getting exposed. Auth

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
BuddyPress 5.1.2 Security Release · BuddyPress.org	MISC	buddypress.org
BuddyPress private data exposure via REST API · Advisory · buddypress/BuddyPress · GitHub	CONFIRM	github.com
Admin: Sanitize external links to activated BP component pages. · buddypress/BuddyPress@3929468 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#)