



CVE-2020-5262

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

Summary

CVE	CVE-2020-5262
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-19 17:15:00 UTC
Updated	2020-03-23 18:15:00 UTC
Description	In EasyBuild before version 4.1.2, the GitHub Personal Access Token (PAT) used by EasyBuild for the GitHub integration f

Risk And Classification

Problem Types: CWE-922

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Easybuild Project	Easybuild	All	All	All	All
Application	Easybuild Project	Easybuild	All	All	All	All

References

Reference

- [censor authorization part of headers before logging ReST API request by boegel · Pull Request #3248 · easybuilders/easybuild-framework · GitHub](#)
- [sync develop with master after release of EasyBuild v4.1.2 by boegel · Pull Request #3249 · easybuilders/easybuild-framework · GitHub](#)
- [GitHub personal access token leaking into temporary EasyBuild \(debug\) logs · Advisory · easybuilders/easybuild-framework · GitHub](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[20269](#) IBM DB2 Multiple Vulnerabilities (6466365)

[982974](#) Python (pip) Security Update for easybuild-framework (GHSA-2wx6-wc87-rmjm)

© [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](#)