CVE-2020-28002

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-28002
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-02 21:15:00 UTC
Updated	2020-11-17 18:01:00 UTC
Description	In SonarQube 8.4.2.36762, an external attacker can achieve authentication bypass through SonarScanner. With an empty

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sonarsource	Sonarqube	8.4.2.36762	All	All	All
Application	Sonarsource	Sonarqube	8.4.2.36762	All	All	All

References

Reference	Source	Link	Tags
SonarQube – Auditando al Auditor – Parte II – CSL	MISC	csl.com.co	Exploit, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730412 SonarSource SonarQube Authentication Bypass Vulnerability (CVE-2020-28002)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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