



CVE-2022-20619

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2022-20619 |
| State | PUBLIC |
| Assigner | jenkinsci-cert@googlegroups.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-01-12 20:15:00 UTC |
| Updated | 2023-11-30 18:43:00 UTC |
| Description | A cross-site request forgery (CSRF) vulnerability in Jenkins Bitbucket Branch Source Plugin 737.vdf9dc06105be and earlier |

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------|-------------------------|-------------------|--------|---------|----------|
| Application | Jenkins | Bitbucket Branch Source | 737.vdf9dc06105be | All | All | All |
| Application | Jenkins | Bitbucket Branch Source | All | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|--|---------------------|
| oss-security - Multiple vulnerabilities in Jenkins and Jenkins plugins | MLIST | www.openwall.com | |
| Jenkins Security Advisory 2022-01-12 | CONFIRM | www.jenkins.io | |
| 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

376410 Jenkins Plugins Multiple Security Vulnerabilities (Jenkins Security Advisory 2022-01-12)

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](#)