



CVE-2020-26939

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

Summary

CVE	CVE-2020-26939
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-02 22:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	In Legion of the Bouncy Castle BC before 1.61 and BC-FJA before 1.0.1.2, attackers can obtain sensitive information about

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Solr	8.8.2	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle	All	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle	All	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-fips-java-api	All	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-fips-java-api	All	All	All	All

References

Reference	Source
Pony Mail!	MLIST
CVE 2020 26939 · bcgit/bc-java Wiki · GitHub	MISC
[solr-issues] 20210525 [jira] [Created] (SOLR-15431) Security vulnerability with Bouncy Castle library within Apache Solr 8.8.2	
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)