CVE-2019-11272

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-11272
State	PUBLIC
Assigner	security@pivotal.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-26 14:15:00 UTC
Updated	2021-06-08 18:21:00 UTC
Description	Spring Security, versions 4.2.x up to 4.2.12, and older unsupported versions support plain text passwords using PlaintextPa

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Pivotal Software	Spring Security	All	All	All	All
Application	Vmware	Spring Security	All	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 1848-1] libspring-security-2.0-java security update	MLIST	lists.debian.or
CVE-2019-11272: PlaintextPasswordEncoder authenticates encoded passwords that are null | Security | Pivotal	CONFIRM	pivotal.io
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

982339 Java (maven) Security Update for org.springframework.security:spring-security-core (GHSA-v33x-prhc-gph5)