CVE-2019-3795

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-3795
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-09 16:29:00 UTC
Updated	2021-11-02 20:18:00 UTC
Description	Spring Security versions 4.2.x prior to 4.2.12, 5.0.x prior to 5.0.12, and 5.1.x prior to 5.1.5 contain an insecure randomness

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
[SECURITY] [DLA 1794-1] libspring-security-2.0-java security update	MLIST
CVE-2019-3795: Insecure Randomness When Using a SecureRandom Instance Constructed by Spring Security | Security | Pivotal	CONFI
Pivotal Spring Security CVE-2019-3795 Security Weakness	BID
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980235 Java (maven) Security Update for org.springframework.security:spring-security-core (GHSA-v2r2-7qm7-jj6v)