



CVE-2020-28923

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

Summary

CVE	CVE-2020-28923
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-03 17:15:00 UTC
Updated	2020-12-07 18:45:00 UTC
Description	An issue was discovered in Play Framework 2.8.0 through 2.8.4. Carefully crafted JSON payloads sent as a form field lead

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lightbend	Play Framework	All	All	All	All

References

Reference	Source	Link	Tags
Play Security Vulnerabilities	MISC	www.playframework.com	Vendor Advisory
Play Framework Security Advisory	CONFIRM	www.playframework.com	Vendor 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.

There are currently no legacy QID mappings associated with this CVE.

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](#)