



CVE-2022-28355

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

Summary

CVE	CVE-2022-28355
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-02 21:15:00 UTC
Updated	2022-04-11 19:34:00 UTC
Description	randomUUID in Scala.js before 1.10.0 generates predictable values.

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Scala-js	Scala.js	All	All	All	All

References

Reference	Source
java.util.UUID.randomUUID() uses an insecure PRNG · Advisory · scala-js/scala-js · GitHub	CO
Announcing Scala.js 1.10.0 - Scala.js	CO
Scala.js should not provide a cryptographically insecure `UUID.randomUUID()` implementation · Issue #4657 · scala-js/scala-js · GitHub	MIS
Releases · scala-js/scala-js · GitHub	MIS
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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

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](#)