



CVE-2017-7252

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

Summary

CVE	CVE-2017-7252
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-03 01:15:00 UTC
Updated	2023-11-13 17:50:00 UTC
Description	bcrypt password hashing in Botan before 2.1.0 does not correctly handle passwords with a length between 57 and 72 characters

Risk And Classification

Problem Types: CWE-319

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Botan Project	Botan	All	All	All	All

References

Reference
Bug 1034591 – VUL-0: CVE-2017-7252: Botan: Botans implementation of bcrypt password hashing scheme truncated longpasswords at 56 characters
Security Advisories — Botan
CVE Program record
NVD vulnerability detail

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](#)