CVE-2016-20013

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-20013
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-19 05:15:00 UTC
Updated	2022-03-03 16:43:00 UTC
Description	sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of service (CPU consumption) because the algo

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sha256crypt Project	Sha256crypt	All	All	All	All
Application	Sha512crypt Project	Sha2512crypt	All	All	All	All
Application	Sha512crypt Project	Sha512crypt	All	All	All	All

References

Reference	Source	Link	Tags
JavaScript is not available.	MISC	twitter.com	
Aaron Toponce : Do Not Use sha256crypt / sha512crypt - They're Dangerous	MISC	pthree.org	
akkadia.org/drepper/SHA-crypt.txt	MISC	akkadia.org	
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.