CVE-2020-5209

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

Summary

CVE	CVE-2020-5209
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-28 18:15:00 UTC
Updated	2020-02-03 18:10:00 UTC
Description	In NetHack before 3.6.5, unknown options starting with -de and -i can cause a buffer overflow resulting in a crash or remote

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nethack	Nethack	All	All	All	All
Application	Nethack	Nethack	All	All	All	All

References

Reference	Sou
command line triggered buffer overruns · NetHack/NetHack@f3def5c · GitHub	MIS
NetHack command line parsing of options starting with -de and -i is subject to a buffer overflow · Advisory · NetHack/NetHack · GitHub	CON
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180781 Debian Security Update for nethack (CVE-2020-5209)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report