



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	Source
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	COM
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)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

Free CVE JSON API cve.report/api

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