CVE-2020-5254

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

Summary

CVE	CVE-2020-5254
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-10 17:15:00 UTC
Updated	2020-03-20 14:51:00 UTC
Description	In NetHack before 3.6.6, some out-of-bound values for the hilite_status option can be exploited. NetHack 3.6.6 resolves this

Risk And Classification

Problem Types: CWE-119

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	Link	Tags
NetHack hilite_status parsing privilege escalation · Advisory · NetHack/NetHack · GitHub	CONFIRM	github.com	Vendor Advisory
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.

Legacy QID Mappings

180674 Debian Security Update for nethack (CVE-2020-5254)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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