



CVE-2020-5214

Published on: 01/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:03 PM UTC

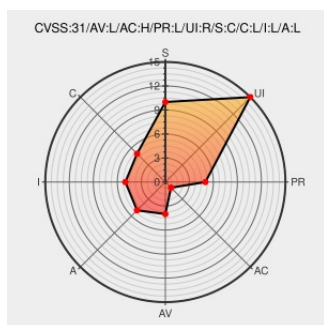
CVE-2020-5214 - advisory for GHSA-p8fw-rq89-xqx6

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Nethack](#) from [Nethack](#) contain the following vulnerability:

In NetHack before 3.6.5, detecting an unknown configuration file option can cause a buffer overflow resulting in a crash or remote code execution/privilege escalation. This vulnerability affects systems that have NetHack installed suid/sgid and shared systems that allow users to upload their own configuration files. Users should upgrade to

NetHack 3.6.5.

CVE-2020-5214 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **NetHack** - NetHack version < 3.6.5

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Description

Tags

Link

NetHack error recovery after syntax error in configuration file is subject to a buffer overflow · Advisory · NetHack/NetHack · GitHub

Third Party Advisory

github.com

text/html

CONFIRM

github.com/NetHack/NetHack/security/advisories/GHSA-p8fw-rq89-xqx6

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

180750 Debian Security Update for nethack (CVE-2020-5214)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:nethack:nethack:*****:.*

cpe:2.3:a:nethack:nethack:*****:.*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →