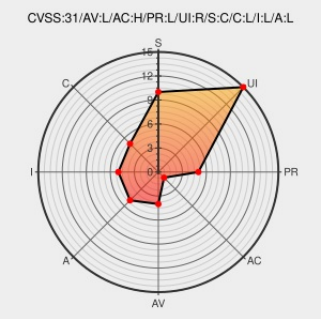
CVE-2020-5213

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

Last Modified on: 03/23/2021 11:24:04 PM UTC

CVE-2020-5213 - advisory for GHSA-rr25-4v34-pr7v

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nethack from Nethack contain the following vulnerability:

In NetHack before 3.6.5, too long of a value for the SYMBOL 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-2020-5213 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 SYMBOL configuration file option 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-rr25-4v34-pr7v

Related QID Numbers

180679 Debian Security Update for nethack (CVE-2020-5213)

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→