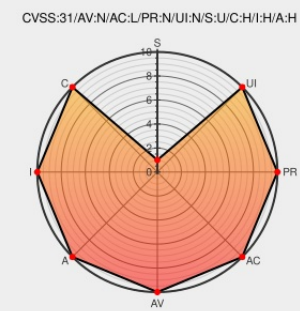
CVE-2019-19905

Published on: 12/19/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19905

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



Certain versions of Nethack from Nethack contain the following vulnerability:

NetHack 3.6.x before 3.6.4 is prone to a buffer overflow vulnerability when reading very long lines from configuration files. This affects systems that have NetHack installed suid/sgid, and shared systems that allow users to upload their own configuration files.

CVE-2019-19905 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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
NetHack 3.6.5: Security Issues	Vendor Advisory, nethack.org, text/html	MISC nethack.org/security/
parse_conf_file fix fix ·	Patch	MISC

NetHack/NetHack@f001de7 · GitHub	github.com text/html	github.com/NetHack/NetHack/commit/f001de79542b8c38b1f8e6d7eaefbbd28ab94b47
NetHack: Privilege escalation/remote code execution/crash in configuration parsing · Advisory · NetHack/NetHack · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/NetHack/NetHack/security/advisories/GHSA-3cm7-rgh5-9pq5
#947005 - nethack: CVE-2019-19905: buffer overflow when parsing config files - Debian Bug report logs	Issue Tracking Patch Third Party Advisory bugs.debian.org text/html	MISC bugs.debian.org/947005
fix potential buffer overflow loading config file · NetHack/NetHack@f4a840a · GitHub	Patch github.com text/html	MISC github.com/NetHack/NetHack/commit/f4a840a48f4bcf11757b3d859e9d53cc9d5ef226

Related QID Numbers

501094 Alpine Linux Security Update for nethack

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→