

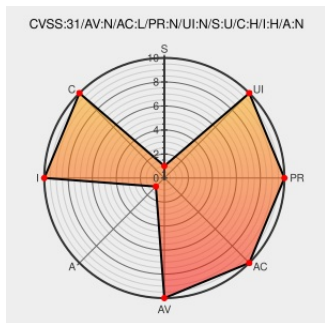


CVE-2021-28918

Published on: 04/01/2021 12:00:00 AM UTC

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2021-28918

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Improper input validation of octal strings in netmask npm package v1.0.6 and below allows unauthenticated remote attackers to perform indeterminate SSRF, RFI, and LFI attacks on many of the dependent packages. A remote unauthenticated attacker can bypass packages relying on netmask to filter IPs and reach critical VPN or LAN hosts.

CVE-2021-28918 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.4 - MEDIUM**

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

CVE References

Description	Tags	Link
Critical netmask networking bug impacts thousands of applications	www.bleepingcomputer.com/text/html	MISC www.bleepingcomputer.com/news/security/critical-netmask-networking-bug-impacts-thousands-of-applications/

Vulnerability in 'netmask' npm Package Affects 280,000 Projects	rootdaemon.com text/html	 MISC rootdaemon.com/2021/03/29/vulnerability-in-netmask-npm-package-affects-280000-projects/
security/SICK-2021-011.md at master · sickcodes/security · GitHub	github.com text/html	 MISC github.com/sickcodes/security/blob/master/advisories/SICK-2021-011.md
GitHub - rs/node-netmask: Parse and lookup IP network blocks	github.com text/html	 MISC github.com/rs/node-netmask
netmask npm package vulnerable to octal input data · CVE-2021-28918 · GitHub Advisory Database · GitHub	github.com text/html	 MISC github.com/advisories/GHSA-pch5-whg9-qr2r
netmask - npm	www.npmjs.com text/html	 MISC www.npmjs.com/package/netmask
CVE-2021-28918 Node.js Vulnerability in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20210528-0010/

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

- [375431](#) Npm Package Netmask Octal Input Data Vulnerability
- [982376](#) Nodejs (npm) Security Update for netmask (GHSA-4c7m-wxvm-r7gc)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netmask Project	Netmask	All	All	All	All
cpe:2.3:a:netmask_project:netmask:*:*:*:*:node.js:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-28918 : Improper input validation of octal strings in netmask npm package v1.0.6 and below allows unauthen... twitter.com/i/web/status/1...	2021-04-01 13:05:32
 /r/opensource	TONIGHT at 7pm EST, Watch the DCG 201 Online Meet Up covering Netmask 0day CVE-2021-28918, Detecting At-Risk Software, Music with Nintendo Switch Joy-Cons & More!	2021-04-16 17:13:23
 /r/NintendoSwitchHacking	TONIGHT at 7pm EST, Watch the DCG 201 Online Meet Up covering Netmask 0day CVE-2021-28918, Detecting At-Risk Software, Music with Nintendo Switch Joy-Cons & More!	2021-04-16 17:11:07
 /r/Defcon	TONIGHT at 7pm EST, Watch the DCG 201 Online Meet Up covering Netmask 0day CVE-2021-28918, Detecting At-Risk Software, Music with Nintendo Switch Joy-Cons & More!	2021-04-16 17:07:55

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)