# CVE Detail – CVE-2021-28918

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.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.99336

## CVSS Scoring

CVSS v3.1 Score: 9.1

Severity: CRITICAL

## Mapped CWE(s)

* CWE-704: Incorrect Type Conversion or Cast

## Affected Products

* cpe:2.3:a:netmask\_project:netmask:\*:\*:\*:\*:\*:node.js:\*:\*