



# CVE-2021-29424

Published on: 03/29/2021 12:00:00 AM UTC

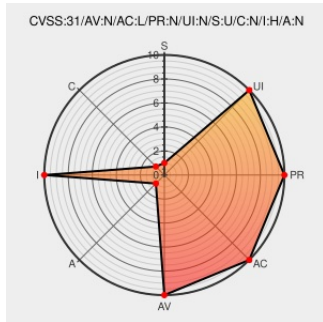
Last Modified on: 06/08/2021 01:52:00 PM UTC

## CVE-2021-29424

Source: Mitre

Source: Nist

Print: PDF



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

The `Net::Netmask` module before 2.0000 for Perl does not properly consider extraneous zero characters at the beginning of an IP address string, which (in some situations) allows attackers to bypass access control that is based on IP addresses.

CVE-2021-29424 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>NONE</b>	<b>PARTIAL</b>	<b>NONE</b>

## CVE References


Description	Tags	Link
Changes - metacpan.org	<a href="#">metacpan.org</a> <a href="#">text/html</a>	<a href="https://metacpan.org/changes/distribution/Net-Netmask#L11-22">MISC metacpan.org/changes/distribution/Net-Netmask#L11-22</a>
[SECURITY] Fedora 33 Update: perl-Net-Netmask-2.0001-1.fc33 -	<a href="#">lists.fedoraproject.org</a>	<a href="#">FEDORA FEDORA-2021-be62be8c7c</a>

package-announce - Fedora Mailing-Lists

text/html


CVE-2021-29424 Perl Vulnerability in NetApp Products | NetApp Product Security

security.netapp.com  
text/html

 CONFIRM  
security.netapp.com/advisory/ntap-20210604-0007/

Security Issues in Perl IP Address distros - House Absolute(ly) Pointless

blog.urth.org  
text/html

 MISC  
blog.urth.org/2021/03/29/security-issues-in-perl-ip-address-distros/

[SECURITY] Fedora 32 Update: perl-Net-Netmask-2.0001-1.fc32 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org  
text/html

 FEDORA FEDORA-2021-c314017fcc

[SECURITY] Fedora 34 Update: perl-Net-Netmask-2.0001-1.fc34 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org  
text/html

 FEDORA FEDORA-2021-3d96cfe6a3

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](mailto:comment@cve.report).

### Related QID Numbers

- [281091](#) Fedora Security Update for Perl-Net-Netmask
- [281391](#) Fedora Security Update for perl (FEDORA-2021-3d96cfe6a3)
- [281392](#) Fedora Security Update for perl (FEDORA-2021-c314017fcc)
- [281393](#) Fedora Security Update for perl (FEDORA-2021-be62be8c7c)

### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Application	<a href="#">Net</a>		netmask_project	net		netmask
Application	<a href="#">Net</a>		netmask_project	net\	\	netmask

cpe:2.3:o:fedoraproject:fedora:32:\*:\*:\*:\*:\*:

cpe:2.3:o:fedoraproject:fedora:33:\*:\*:\*:\*:\*:

cpe:2.3:o:fedoraproject:fedora:34:\*:\*:\*:\*:\*:

cpe:2.3:a:net::netmask\_project:net::netmask:\*:\*:\*:

cpe:2.3:a:net\:\:netmask\_project:net\:\:netmask:\*:\*:\*:

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2021 [Twitter](#) [News](#) |

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](#)**