



# CVE-2020-11985

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-11985
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-08-07 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:15:00 UTC
<b>Description</b>	IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remo

## Risk And Classification

**Problem Types:** CWE-345

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All

## References

Reference	Source	Link	Ta
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
CVE-2020-11985 Apache HTTP Server Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
[SECURITY] Fedora 32 Update: httpd-2.4.46-1.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	

Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	MISC	<a href="http://httpd.apache.org">httpd.apache.org</a>	Ve
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
[SECURITY] Fedora 31 Update: httpd-2.4.46-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Apache: Multiple vulnerabilities (GLSA 202008-04) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Tr
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
[SECURITY] Fedora 32 Update: httpd-2.4.46-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Oracle Critical Patch Update Advisory - January 2021	MISC	<a href="http://www.oracle.com">www.oracle.com</a>	
[SECURITY] Fedora 31 Update: httpd-2.4.46-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[296072](#) Oracle Solaris 11.4 Support Repository Update (SRU) 25.75.3 Missing (CPUJUL2020)

[376846](#) IBM Hypertext Transfer Protocol (HTTP) Server Spoofing Vulnerabilities (6324789)

© [CVE.report](https://cve.report) 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)