

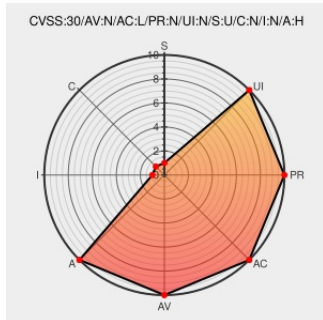


CVE-2018-8011

Published on: 07/18/2018 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:01:00 AM UTC

CVE-2018-8011

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

Certain versions of [Http Server](#) from [Apache](#) contain the following vulnerability:

By specially crafting HTTP requests, the mod_md challenge handler would dereference a NULL pointer and cause the child process to segfault. This could be used to DoS the server. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.33).

CVE-2018-8011 has been assigned by [security@apache.org](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Apache Software Foundation](#) - [Apache HTTP Server](#) version **Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.33)**

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/ison/

	text/html	/websites/staging/httpd/trunk/content: ./ security/json/
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073139 [12/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210606 svn commit: r1075470 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2020-13938.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073140 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/cvejsontohtml.py security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20200401 svn commit: r1058587 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
July 2018 Apache HTTP Server Vulnerabilities in NetApp Products NetApp Product Security	Third Party Advisory security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20180926-0007/
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20190815 svn commit: r1048743 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073149 [12/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20190815 svn commit: r1048742 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073149 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/
httpd 2.4 vulnerabilities - The Apache HTTP Server Project	Vendor Advisory httpd.apache.org text/html	CONFIRM httpd.apache.org/security/vulnerabilities_24.html#CVE-2018-8011
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1888194 [12/13] - /httpd/site/trunk/content/security/json/
Apache HTTPD Null Pointer Dereference in mod_md Lets Remote Users Deny Service - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTrack 1041401
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073143 [3/3] - in /websites/staging/httpd/trunk/content: ./ security/
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20200401 svn commit: r1058586 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html

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.

500014 Alpine Linux Security Update for apache2

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.4.33	All	All	All
Application	Apache	Http Server	2.4.33	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All

```
cpe:2.3:a:apache:http_server:2.4.33:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:2.4.33:*:*:*:*:*:*:
```

```
cpe:2.3:a:netapp:cloud_backup:-:*:*:*:*:*:
```

```
cpe:2.3:a:netapp:cloud_backup:-:*:*:*:*:*:
```

Discovery Credit

The issue was discovered by Daniel Caminada .

[← Previous ID](#)

Next ID→

© 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