CVE-2017-15715

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-15715
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-26 15:29:00 UTC
Updated	2023-11-07 02:40:00 UTC
Description	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicic

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Netapp	Clustered Data Ontap	-	All	All	All
Operating System	Netapp	Clustered Data Ontap	-	All	All	All
Application	Netapp	Santricity Cloud Connector	-	All	All	All
Application	Netapp	Santricity Cloud Connector	-	All	All	All

Application	Netapp	Storagegrid	-	All	All	All
Application	Netapp	Storagegrid	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.4	All	All	All
Operating System	Redhat	Enterprise Linux	7.5	All	All	All
Operating System	Redhat	Enterprise Linux	7.6	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.4	All	All	All
Operating System	Redhat	Enterprise Linux	7.5	All	All	All
Operating System	Redhat	Enterprise Linux	7.6	All	All	All

References

Reference	Sourc
Pony Mail!	
Pony Mail!	
Pony Mail!	
Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	
Pony Mail!	
Red Hat Customer Portal	REDH
Pony Mail!	MLIST
Debian -- Security Information -- DSA-4164-1 apache2	DEBIA
oss-security - CVE-2017-15715: <FilesMatch> bypass with a trailing newline in the file name	MLIST
Pony Mail!	
Red Hat Customer Portal	REDH
[R1] Tenable.sc 5.13.0 Fixes Multiple Third-Party Vulnerabilities - Security Advisory | Tenable®	CONF
Pony Mail!	
March 2018 Apache HTTP Server Vulnerabilities in NetApp Products | NetApp Product Security	CONF
Pony Mail!	MLIST
Pony Mail!	

Red Hat Customer Portal	REDH
Pony Mail!	MLIST
Pony Mail!	
Document Display | HPE Support Center	CONF
USN-3627-2: Apache HTTP Server vulnerabilities | Ubuntu security notices | Ubuntu	UBUN
USN-3627-1: Apache HTTP Server vulnerabilities | Ubuntu security notices | Ubuntu	UBUN
Pony Mail!	MLIST
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	CONF
Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	
Pony Mail!	
Apache HTTPD May Let Remote Users Bypass 'FilesMatch' Directive Security Restrictions on the Target System - SecurityTracker	SECT
Pony Mail!	MLIST
CVE-2017-15715 - Apache HTTP Server - FilesMatch bypass with a trailing newline at the end of the file name - Security | Elar Lang	MISC
Pony Mail!	MLIST
Pony Mail!	
Pony Mail!	MLIST
Apache HTTP Server CVE-2017-15715 Remote Security Bypass Vulnerability	BID
Pony Mail!	MLIST
Pony Mail!	
Pony Mail!	MLIST
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

377516 Alibaba Cloud Linux Security Update for httpd (ALINUX2-SA-2020:0165)

500013 Alpine Linux Security Update for apache2

503704 Alpine Linux Security Update for apache2

© 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 registred 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