



CVE-2017-12171

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

Summary

CVE	CVE-2017-12171
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-26 17:29:00 UTC
Updated	2023-02-12 23:27:00 UTC
Description	A regression was found in the Red Hat Enterprise Linux 6.9 version of httpd 2.2.15-60, causing comments in the "Allow" an

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.2.15-60	All	All	All
Application	Apache	Http Server	2.2.15-60	All	All	All
Operating System	Redhat	Enterprise Linux	6.9	All	All	All
Operating System	Redhat	Enterprise Linux	6.9	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

References

Reference
Apache HTTP Server CVE-2017-12171 Security Bypass Vulnerability
CVE-2017-12171 - Red Hat Customer Portal
1493056 – (CVE-2017-12171) CVE-2017-12171 httpd: # character matches all IPs
Apache HTTPD on Red Hat Enterprise Linux Configuration Parsing Error May Let Remote Users Bypass Security Restrictions - SecurityTrack

Red Hat Customer Portal
1493056 – (CVE-2017-12171) CVE-2017-12171 httpd: # character matches all IPs
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
Legacy QID Mappings
378145 Virtuozzo Linux Security Update for mod_ssl (VZLSA-2017:2972)

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)