



CVE-2015-7519

Published on: 01/08/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:11 PM UTC

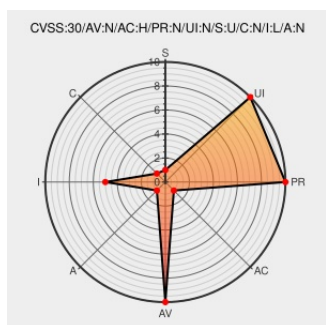
CVE-2015-7519

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Phusion Passenger](#) from [Phusionpassenger](#) contain the following vulnerability:

agent/Core/Controller/SendRequest.cpp in Phusion Passenger before 4.0.60 and 5.0.x before 5.0.22, when used in Apache integration mode or in standalone mode without a filtering proxy, allows remote attackers to spoof headers passed to applications by using an _ (underscore) character instead of a - (dash) character in an HTTP header, as demonstrated by an X_User header.

CVE-2015-7519 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as [LOW](#) severity.

CVSS3 Score: [3.7 - LOW](#)

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

CVSS2 Score: [4.3 - MEDIUM](#)

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

CVE References

Description	Tags	Link
oss-security - CVE-2015-7519: Phusion Passenger	www.openwall.com text/html	MLIST [oss-security] 20151207 CVE-2015-7519: Phusion Passenger Header overwriting issue

Header overwriting issue

CVE-2015-7519 - Header
Overwriting Passenger
Vulnerability | Puppet

[puppet.com](#)[text/html](#) [CONFIRM puppet.com/security/cve/passenger-dec-2015-security-fixes](#)

[security-announce] SUSE-
SU-2015:2337-1: important:
Security update for

[lists.opensuse.org](#)[text/html](#) [SUSE SUSE-SU-2015:2337](#)

oss-security - injecting
environment variables into
Phusion Passenger (CVE-
2015-7519)

[www.openwall.com](#)[text/html](#) [MLIST \[oss-security\] 20151207 injecting environment variables into Phusion Passenger \(CVE-2015-7519\)](#)

[SECURITY] [DLA 1399-1]
ruby-passenger security
update

[lists.debian.org](#)[text/html](#) [MLIST \[debian-lts-announce\] 20180627 \[SECURITY\] \[DLA 1399-1\] ruby-passenger security update](#)

Fix CVE-2015-7519 header
collision vulnerability ·
phusion/passenger@ddb8ecc
· GitHub

[github.com](#)[text/html](#) [CONFIRM github.com/phusion/passenger/commit/ddb8ecc4ebf260e4967f57f271d4f5761abeac3e](#)

Security advisory: CVE-2015-
7519 header overwriting
(medium severity)

[Vendor Advisory](#)[blog.phusion.nl](#)[text/html](#) [CONFIRM blog.phusion.nl/2015/12/07/cve-2015-7519/](#)

Bug 956281 – VUL-0: CVE-
2015-7519: rubygem-
passenger: Passenger is not
filtering environment like
apache is doing

[bugzilla.suse.com](#)[text/html](#) [CONFIRM bugzilla.suse.com/show_bug.cgi?id=956281](#)

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phusionpassenger	Phusion Passenger	5.0.0	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.0	beta1	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.0	beta2	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.0	beta3	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.0	rc1	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.0	rc2	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.1	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.10	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.11	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.12	All	All	All

Application	Phusionpassenger	Phusion Passenger	5.0.20	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.21	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.3	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.4	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.5	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.6	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.7	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.8	All	All	All
Application	Phusionpassenger	Phusion Passenger	5.0.9	All	All	All
Application	Phusionpassenger	Phusion Passenger	All	All	All	All
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:beta1:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:beta2:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:beta3:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:rc1:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:rc2:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.1:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.10:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.11:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.12:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.13:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.14:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.15:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.16:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.17:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.18:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.19:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.2:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.20:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.21:*:*:*:*:*:						
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.3:*:*:*:*:*:						

cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.4:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.5:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.6:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.7:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.8:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.9:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:beta1:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:beta2:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:beta3:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:rc1:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.0:rc2:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.1:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.10:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.11:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.12:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.13:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.14:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.15:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.16:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.17:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.18:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.19:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.2:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.20:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.21:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.3:*****:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.4:*****:

cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.5:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.6:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.7:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.8:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.9:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:*:*:*:*:*:

cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.5:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.6:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.7:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.8:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.9:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:*:*:*:*:*:

cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.5:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.6:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.7:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.8:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.9:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:*:*:*:*:*:

cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.5:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.6:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.7:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.8:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.9:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:*:*:*:*:*:

cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.5:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.6:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.7:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.8:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.9:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:*:*:*:*:*:

cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.5:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.6:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.7:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.8:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:5.0.9:*:*:*:*:*:
cpe:2.3:a:phusionpassenger:phusion_passenger:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← 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