

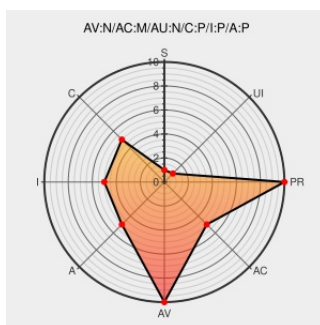


CVE-2013-4407

Published on: 11/23/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:14 AM UTC

CVE-2013-4407

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

Certain versions of [Http-body](#) from [Http-body Project](#) contain the following vulnerability:

HTTP::Body::Multipart in the HTTP-Body 1.08, 1.17, and earlier module for Perl uses the part of the uploaded file's name after the first "." character as the suffix of a temporary file, which makes it easier for remote attackers to conduct attacks by leveraging subsequent behavior that may assume the suffix is well-formed.

CVE-2013-4407 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

[security-announce] openSUSE-SU-2014:0433-1: important: perl-HTTP-Body:

[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2014:0433](#)

Debian -- Security Information -- DSA-2801-1 libhttp-body-perl

[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-2801](#)

#721634 - libhttp-body-perl: CVE-2013-4407: HTTP::Body::Multipart critical security bug - Debian Bug report logs

[bugs.debian.org](#)
[text/html](#)

[CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=721634](#)

By selecting these links, you may be leaving CVEreport workspace. 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	Http-body Project	Http-body	0.01	All	All	All
Application	Http-body Project	Http-body	0.03	All	All	All
Application	Http-body Project	Http-body	0.2	All	All	All
Application	Http-body Project	Http-body	0.4	All	All	All
Application	Http-body Project	Http-body	0.5	All	All	All
Application	Http-body Project	Http-body	0.6	All	All	All
Application	Http-body Project	Http-body	0.7	All	All	All
Application	Http-body Project	Http-body	0.8	All	All	All
Application	Http-body Project	Http-body	0.9	All	All	All
Application	Http-body Project	Http-body	1.00	All	All	All
Application	Http-body Project	Http-body	1.01	All	All	All
Application	Http-body Project	Http-body	1.02	All	All	All
Application	Http-body Project	Http-body	1.03	All	All	All
Application	Http-body Project	Http-body	1.04	All	All	All
Application	Http-body Project	Http-body	1.05	All	All	All
Application	Http-body Project	Http-body	1.06	All	All	All
Application	Http-body Project	Http-body	1.07	All	All	All
Application	Http-body Project	Http-body	1.08	All	All	All
Application	Http-body Project	Http-body	1.09	All	All	All
Application	Http-body Project	Http-body	1.10	All	All	All
Application	Http-body Project	Http-body	1.11	All	All	All
Application	Http-body Project	Http-body	1.12	All	All	All
Application	Http-body Project	Http-body	1.14	All	All	All
Application	Http-body Project	Http-body	1.15	All	All	All
Application	Http-body Project	Http-body	1.16	All	All	All
Application	Http-body Project	Http-body	0.01	All	All	All
Application	Http-body Project	Http-body	0.03	All	All	All
Application	Http-body Project	Http-body	0.2	All	All	All
Application	Http-body Project	Http-body	0.4	All	All	All
Application	Http-body Project	Http-body	0.5	All	All	All
Application	Http-body Project	Http-body	0.6	All	All	All

Application	Http-body Project	Http-body	0.0	All	All	All
Application	Http-body Project	Http-body	0.7	All	All	All
Application	Http-body Project	Http-body	0.8	All	All	All
Application	Http-body Project	Http-body	0.9	All	All	All
Application	Http-body Project	Http-body	1.00	All	All	All
Application	Http-body Project	Http-body	1.01	All	All	All
Application	Http-body Project	Http-body	1.02	All	All	All
Application	Http-body Project	Http-body	1.03	All	All	All
Application	Http-body Project	Http-body	1.04	All	All	All
Application	Http-body Project	Http-body	1.05	All	All	All
Application	Http-body Project	Http-body	1.06	All	All	All
Application	Http-body Project	Http-body	1.07	All	All	All
Application	Http-body Project	Http-body	1.08	All	All	All
Application	Http-body Project	Http-body	1.09	All	All	All
Application	Http-body Project	Http-body	1.10	All	All	All
Application	Http-body Project	Http-body	1.11	All	All	All
Application	Http-body Project	Http-body	1.12	All	All	All
Application	Http-body Project	Http-body	1.14	All	All	All
Application	Http-body Project	Http-body	1.15	All	All	All
Application	Http-body Project	Http-body	1.16	All	All	All
Application	Http-body Project	Http-body	All	All	All	All
cpe:2.3:a:http-body_project:http-body:0.01:*****:						
cpe:2.3:a:http-body_project:http-body:0.03:*****:						
cpe:2.3:a:http-body_project:http-body:0.2:*****:						
cpe:2.3:a:http-body_project:http-body:0.4:*****:						
cpe:2.3:a:http-body_project:http-body:0.5:*****:						
cpe:2.3:a:http-body_project:http-body:0.6:*****:						
cpe:2.3:a:http-body_project:http-body:0.7:*****:						
cpe:2.3:a:http-body_project:http-body:0.8:*****:						
cpe:2.3:a:http-body_project:http-body:0.9:*****:						
cpe:2.3:a:http-body_project:http-body:1.00:*****:						
cpe:2.3:a:http-body_project:http-body:1.01:*****:						
cpe:2.3:a:http-body_project:http-body:1.02:*****:						

cpe:2.3:a:http-body_project:http-body:1.03:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.04:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.05:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.06:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.07:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.08:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.09:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.10:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.11:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.12:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.14:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.15:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.16:*****:.*:
cpe:2.3:a:http-body_project:http-body:0.01:*****:.*:
cpe:2.3:a:http-body_project:http-body:0.03:*****:.*:
cpe:2.3:a:http-body_project:http-body:0.2:*****:.*:
cpe:2.3:a:http-body_project:http-body:0.4:*****:.*:
cpe:2.3:a:http-body_project:http-body:0.5:*****:.*:
cpe:2.3:a:http-body_project:http-body:0.6:*****:.*:
cpe:2.3:a:http-body_project:http-body:0.7:*****:.*:
cpe:2.3:a:http-body_project:http-body:0.8:*****:.*:
cpe:2.3:a:http-body_project:http-body:0.9:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.00:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.01:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.02:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.03:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.04:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.05:*****:.*:

cpe:2.3:a:http-body_project:http-body:1.06:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.07:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.08:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.09:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.10:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.11:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.12:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.14:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.15:*****:.*:
cpe:2.3:a:http-body_project:http-body:1.16:*****:.*:
cpe:2.3:a:http-body_project:http-body:*****:.*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)