



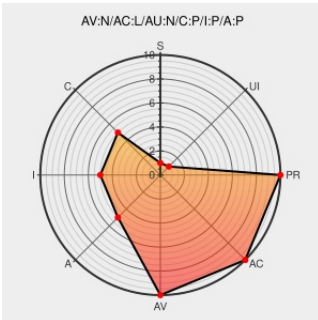
Last Modified on: 03/23/2021 11:25:24 PM UTC

CVE-2009-3287

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Thin](#) from [Macournoyer](#) contain the following vulnerability:

lib/thin/connection.rb in Thin web server before 1.2.4 relies on the X-Forwarded-For header to determine the IP address of the client, which allows remote attackers to spoof the IP address and hide activities via a modified X-Forwarded-For header.

CVE-2009-3287 has been assigned by  cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
oss-security - CVE request(?): Thin: Client IP spoofing	www.openwall.com text/html	 MLIST [oss-security] 20090912 CVE request(?): Thin: Client IP spoofing
CHANGELOG at master from macournoyer's thin - GitHub	github.com text/html	 CONFIRM github.com/macournoyer/thin/blob/master/CHANGELOG
Commit 7bd027914c5ffd36bb408ef47dc749de3b6e063a to macournoyer's thin - GitHub	Patch github.com text/html	 CONFIRM github.com/macournoyer/thin/commit/7bd027914c5ffd36bb408ef47dc749de3b6e063a

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	Macournoyer	Thin	0.4.0	All	All	All
Application	Macournoyer	Thin	0.4.1	All	All	All
Application	Macournoyer	Thin	0.5.0	All	All	All
Application	Macournoyer	Thin	0.5.1	All	All	All
Application	Macournoyer	Thin	0.5.2	All	All	All
Application	Macournoyer	Thin	0.5.3	All	All	All
Application	Macournoyer	Thin	0.5.4	All	All	All
Application	Macournoyer	Thin	0.6.0	All	All	All
Application	Macournoyer	Thin	0.6.3	All	All	All
Application	Macournoyer	Thin	0.6.4	All	All	All
Application	Macournoyer	Thin	0.7.0	All	All	All
Application	Macournoyer	Thin	0.7.1	All	All	All
Application	Macournoyer	Thin	0.8.0	All	All	All
Application	Macournoyer	Thin	0.8.1	All	All	All
Application	Macournoyer	Thin	0.8.2	All	All	All
Application	Macournoyer	Thin	1.0.0	All	All	All
Application	Macournoyer	Thin	1.1.0	All	All	All
Application	Macournoyer	Thin	1.1.1	All	All	All
Application	Macournoyer	Thin	1.2.0	All	All	All
Application	Macournoyer	Thin	1.2.1	All	All	All
Application	Macournoyer	Thin	0.4.0	All	All	All
Application	Macournoyer	Thin	0.4.1	All	All	All
Application	Macournoyer	Thin	0.5.0	All	All	All
Application	Macournoyer	Thin	0.5.1	All	All	All
Application	Macournoyer	Thin	0.5.2	All	All	All
Application	Macournoyer	Thin	0.5.3	All	All	All
Application	Macournoyer	Thin	0.5.4	All	All	All
Application	Macournoyer	Thin	0.6.0	All	All	All
Application	Macournoyer	Thin	0.6.3	All	All	All
Application	Macournoyer	Thin	0.6.4	All	All	All
Application	Macournoyer	Thin	0.7.0	All	All	All

Application	Macournoyer	Thin	0.7.1	All	All	All
Application	Macournoyer	Thin	0.8.0	All	All	All
Application	Macournoyer	Thin	0.8.1	All	All	All
Application	Macournoyer	Thin	0.8.2	All	All	All
Application	Macournoyer	Thin	1.0.0	All	All	All
Application	Macournoyer	Thin	1.1.0	All	All	All
Application	Macournoyer	Thin	1.1.1	All	All	All
Application	Macournoyer	Thin	1.2.0	All	All	All
Application	Macournoyer	Thin	1.2.1	All	All	All
Application	Macournoyer	Thin	All	All	All	All
cpe:2.3:a:macournoyer:thin:0.4.0:*****:						
cpe:2.3:a:macournoyer:thin:0.4.1:*****:						
cpe:2.3:a:macournoyer:thin:0.5.0:*****:						
cpe:2.3:a:macournoyer:thin:0.5.1:*****:						
cpe:2.3:a:macournoyer:thin:0.5.2:*****:						
cpe:2.3:a:macournoyer:thin:0.5.3:*****:						
cpe:2.3:a:macournoyer:thin:0.5.4:*****:						
cpe:2.3:a:macournoyer:thin:0.6.0:*****:						
cpe:2.3:a:macournoyer:thin:0.6.3:*****:						
cpe:2.3:a:macournoyer:thin:0.6.4:*****:						
cpe:2.3:a:macournoyer:thin:0.7.0:*****:						
cpe:2.3:a:macournoyer:thin:0.7.1:*****:						
cpe:2.3:a:macournoyer:thin:0.8.0:*****:						
cpe:2.3:a:macournoyer:thin:0.8.1:*****:						
cpe:2.3:a:macournoyer:thin:0.8.2:*****:						
cpe:2.3:a:macournoyer:thin:1.0.0:*****:						
cpe:2.3:a:macournoyer:thin:1.1.0:*****:						
cpe:2.3:a:macournoyer:thin:1.1.1:*****:						
cpe:2.3:a:macournoyer:thin:1.2.0:*****:						
cpe:2.3:a:macournoyer:thin:1.2.1:*****:						

cpe:2.3:a:macournoyer:thin:0.4.0:*****:
cpe:2.3:a:macournoyer:thin:0.4.1:*****:
cpe:2.3:a:macournoyer:thin:0.5.0:*****:
cpe:2.3:a:macournoyer:thin:0.5.1:*****:
cpe:2.3:a:macournoyer:thin:0.5.2:*****:
cpe:2.3:a:macournoyer:thin:0.5.3:*****:
cpe:2.3:a:macournoyer:thin:0.5.4:*****:
cpe:2.3:a:macournoyer:thin:0.6.0:*****:
cpe:2.3:a:macournoyer:thin:0.6.3:*****:
cpe:2.3:a:macournoyer:thin:0.6.4:*****:
cpe:2.3:a:macournoyer:thin:0.7.0:*****:
cpe:2.3:a:macournoyer:thin:0.7.1:*****:
cpe:2.3:a:macournoyer:thin:0.8.0:*****:
cpe:2.3:a:macournoyer:thin:0.8.1:*****:
cpe:2.3:a:macournoyer:thin:0.8.2:*****:
cpe:2.3:a:macournoyer:thin:1.0.0:*****:
cpe:2.3:a:macournoyer:thin:1.1.0:*****:
cpe:2.3:a:macournoyer:thin:1.1.1:*****:
cpe:2.3:a:macournoyer:thin:1.2.0:*****:
cpe:2.3:a:macournoyer:thin:1.2.1:*****:
cpe:2.3:a:macournoyer:thin:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

