

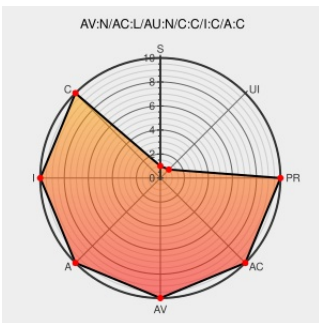


CVE-2014-3954

Published on: 10/27/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:47 PM UTC

CVE-2014-3954

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

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

Stack-based buffer overflow in rtsold in FreeBSD 9.1 through 10.1-RC2 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via crafted DNS parameters in a router advertisement message.

CVE-2014-3954 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

FreeBSD Buffer Overflow in rtsold(8) IPv6 Router Solicitation Daemon May Let Remote Users Execute Arbitrary Code - SecurityTracker

www.securitytracker.com
[text/html](#)

[SECTrack](#)
1031098

[Patch](#)
www.freebsd.org
[text/plain](#)

[FREEBSD](#)
[FreeBSD-SA-14:20](#)

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
Operating System	Freebsd	Freebsd	10.0	All	All	All
Operating System	Freebsd	Freebsd	10.0	rc1	All	All
Operating System	Freebsd	Freebsd	10.0	rc2	All	All
Operating System	Freebsd	Freebsd	10.1	All	All	All
Operating System	Freebsd	Freebsd	10.1	rc1	All	All
Operating System	Freebsd	Freebsd	10.1	rc2	All	All
Operating System	Freebsd	Freebsd	9.1	All	All	All
Operating System	Freebsd	Freebsd	9.1	p4	All	All
Operating System	Freebsd	Freebsd	9.1	p5	All	All
Operating System	Freebsd	Freebsd	9.2	-	All	All
Operating System	Freebsd	Freebsd	9.2	prerelease	All	All
Operating System	Freebsd	Freebsd	9.2	rc1	All	All
Operating System	Freebsd	Freebsd	9.2	rc2	All	All
Operating System	Freebsd	Freebsd	9.3	All	All	All
Operating System	Freebsd	Freebsd	9.3	rc1	All	All
Operating System	Freebsd	Freebsd	9.3	rc2	All	All
Operating System	Freebsd	Freebsd	10.0	All	All	All
Operating System	Freebsd	Freebsd	10.0	rc1	All	All
Operating System	Freebsd	Freebsd	10.0	rc2	All	All
Operating System	Freebsd	Freebsd	10.1	All	All	All
Operating System	Freebsd	Freebsd	10.1	rc1	All	All
Operating System	Freebsd	Freebsd	10.1	rc2	All	All

Operating System	Freebsd	Freebsd	9.0	rc1	All	All
Operating System	Freebsd	Freebsd	9.1	All	All	All
Operating System	Freebsd	Freebsd	9.1	p4	All	All
Operating System	Freebsd	Freebsd	9.1	p5	All	All
Operating System	Freebsd	Freebsd	9.2	-	All	All
Operating System	Freebsd	Freebsd	9.2	prerelease	All	All
Operating System	Freebsd	Freebsd	9.2	rc1	All	All
Operating System	Freebsd	Freebsd	9.2	rc2	All	All
Operating System	Freebsd	Freebsd	9.3	All	All	All
Operating System	Freebsd	Freebsd	9.3	rc1	All	All
Operating System	Freebsd	Freebsd	9.3	rc2	All	All
cpe:2.3:o:freebsd:freebsd:10.0:*****:						
cpe:2.3:o:freebsd:freebsd:10.0:rc1:*****:						
cpe:2.3:o:freebsd:freebsd:10.0:rc2:*****:						
cpe:2.3:o:freebsd:freebsd:10.1:*****:						
cpe:2.3:o:freebsd:freebsd:10.1:rc1:*****:						
cpe:2.3:o:freebsd:freebsd:10.1:rc2:*****:						
cpe:2.3:o:freebsd:freebsd:9.1:*****:						
cpe:2.3:o:freebsd:freebsd:9.1:p4:*****:						
cpe:2.3:o:freebsd:freebsd:9.1:p5:*****:						
cpe:2.3:o:freebsd:freebsd:9.2:-:*****:						
cpe:2.3:o:freebsd:freebsd:9.2:prerelease:*****:						
cpe:2.3:o:freebsd:freebsd:9.2:rc1:*****:						
cpe:2.3:o:freebsd:freebsd:9.2:rc2:*****:						
cpe:2.3:o:freebsd:freebsd:9.3:*****:						
cpe:2.3:o:freebsd:freebsd:9.3:rc1:*****:						

cpe:2.3:o:freebsd:freebsd:9.3:rc2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:10.0:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:10.0:rc1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:10.0:rc2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:10.1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:10.1:rc1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:10.1:rc2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:9.1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:9.1:p4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:9.1:p5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:9.2:-:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:9.2:prerelease:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:9.2:rc1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:9.2:rc2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:9.3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:9.3:rc1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:9.3:rc2:~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)