



CVE-2001-1401

Published on: 09/10/2001 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:18 PM UTC

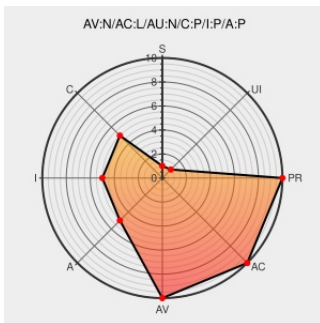
CVE-2001-1401

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Bugzilla before 2.14 does not properly restrict access to confidential bugs, which could allow Bugzilla users to bypass viewing permissions via modified bug id parameters in (1) process_bug.cgi, (2) show_activity.cgi, (3) showvotes.cgi, (4) showdependencytree.cgi, (5) showdependencygraph.cgi, (6) showattachment.cgi, or (7)

describecomponents.cgi.

CVE-2001-1401 has been assigned by [M](#) 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
'Security Advisory for Bugzilla v2.13 and older' - MARC	marc.info text/html	BUGTRAQ 20010829 Security Advisory for Bugzilla v2.13 and older
39527 - showvotes.cgi doesn't check viewing permissions	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=39527
39531 - showdependencytree.cgi doesn't check viewing permissions	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=39531
39533 - showdependencygraph.cgi doesn't check viewing permissions	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=39533
82781 - describecomponents.cgi doesn't check viewing permissions	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=82781

70189 - showattachment.cgi doesn't check viewing permissions

bugzilla.mozilla.org
text/html

CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=70189

39524 - process_bug.cgi doesn't check viewing permissions

bugzilla.mozilla.org
text/html

CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=39524

39526 - show_activity.cgi doesn't check viewing permissions

bugzilla.mozilla.org
text/html

CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=39526

redhat.com | Red Hat Support

Patch
Vendor Advisory
www.redhat.com
text/html

REDHAT RHSA-2001:107

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	Mozilla	Bugzilla	2.10	All	All	All
Application	Mozilla	Bugzilla	2.12	All	All	All
Application	Mozilla	Bugzilla	2.14	All	All	All
Application	Mozilla	Bugzilla	2.4	All	All	All
Application	Mozilla	Bugzilla	2.6	All	All	All
Application	Mozilla	Bugzilla	2.8	All	All	All
Application	Mozilla	Bugzilla	2.10	All	All	All
Application	Mozilla	Bugzilla	2.12	All	All	All
Application	Mozilla	Bugzilla	2.14	All	All	All
Application	Mozilla	Bugzilla	2.4	All	All	All
Application	Mozilla	Bugzilla	2.6	All	All	All
Application	Mozilla	Bugzilla	2.8	All	All	All

cpe:2.3:a:mozilla:bugzilla:2.10:*:*:*:*:*:

cpe:2.3:a:mozilla:bugzilla:2.12:*:*:*:*:*:

cpe:2.3:a:mozilla:bugzilla:2.14:*:*:*:*:*:

cpe:2.3:a:mozilla:bugzilla:2.4:*:*:*:*:*:

cpe:2.3:a:mozilla:bugzilla:2.6:*:*:*:*:*:

cpe:2.3:a:mozilla:bugzilla:2.8:*:*:*:*:*:

cpe:2.3:a:mozilla:bugzilla:2.10:*****:	
cpe:2.3:a:mozilla:bugzilla:2.12:*****:	
cpe:2.3:a:mozilla:bugzilla:2.14:*****:	
cpe:2.3:a:mozilla:bugzilla:2.4:*****:	
cpe:2.3:a:mozilla:bugzilla:2.6:*****:	
cpe:2.3:a:mozilla:bugzilla:2.8:*****:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID →