

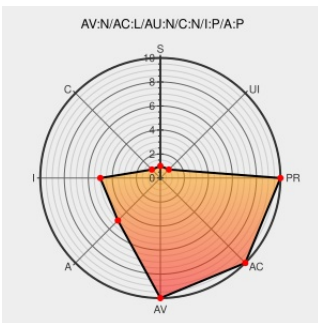


CVE-2011-4675

Published on: 12/05/2011 12:00:00 AM UTC

Last Modified on: 06/25/2021 02:19:00 PM UTC

CVE-2011-4675

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

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

The pathname canonicalization functionality in `io/filesystem/filesystem.cc` in [Widelands](#) before 15.1 expands leading `~` (tilde) characters to home-directory pathnames but does not restrict use of these characters in strings received from the network, which might allow remote attackers to conduct absolute path traversal attacks and overwrite arbitrary files via a `~` in a pathname that is used for a file transfer in an Internet game, a different vulnerability than CVE-2011-1932.

CVE-2011-4675 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF widelands-filesystem-file-overwrite\(71626\)](#)

`~widelands-dev/widelands/build-15` : revision 5021

[Patch](#)
[bazaar.launchpad.net](#)
[text/xml](#)

[CONFIRM](#)
[bazaar.launchpad.net/~widelands-dev/widelands/build-15/revision/5021](#)

#617960 - widelands: potential security issue in internet games - Debian Bug report logs

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

[CONFIRM](#) [bugs.debian.org/cgi-bin/bugreport.cgi?bug=617960](#)

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	Widelands	Widelands	-	build1	All	All
Application	Widelands	Widelands	-	build10	All	All
Application	Widelands	Widelands	-	build10_release_candidate	All	All
Application	Widelands	Widelands	-	build11	All	All
Application	Widelands	Widelands	-	build11_release_candidate	All	All
Application	Widelands	Widelands	-	build12	All	All
Application	Widelands	Widelands	-	build12_release_candidate	All	All
Application	Widelands	Widelands	-	build13	All	All
Application	Widelands	Widelands	-	build13_release_candidate	All	All
Application	Widelands	Widelands	-	build13_release_candidate2	All	All
Application	Widelands	Widelands	-	build14	All	All
Application	Widelands	Widelands	-	build14_release_candidate	All	All
Application	Widelands	Widelands	-	build2	All	All
Application	Widelands	Widelands	-	build3	All	All
Application	Widelands	Widelands	-	build4	All	All
Application	Widelands	Widelands	-	build5	All	All
Application	Widelands	Widelands	-	build6	All	All
Application	Widelands	Widelands	-	build7	All	All
Application	Widelands	Widelands	-	build8	All	All
Application	Widelands	Widelands	-	build9	All	All
Application	Widelands	Widelands	1	All	All	All
Application	Widelands	Widelands	10	All	All	All
Application	Widelands	Widelands	11	All	All	All
Application	Widelands	Widelands	12	All	All	All
Application	Widelands	Widelands	13	All	All	All
Application	Widelands	Widelands	14	All	All	All
Application	Widelands	Widelands	15	All	All	All
Application	Widelands	Widelands	2	All	All	All
Application	Widelands	Widelands	3	All	All	All

Application	Widelands	Widelands	4	All	All	All
Application	Widelands	Widelands	5	All	All	All
Application	Widelands	Widelands	6	All	All	All
Application	Widelands	Widelands	7	All	All	All
Application	Widelands	Widelands	8	All	All	All
Application	Widelands	Widelands	9	All	All	All
Application	Widelands	Widelands	9.5	All	All	All
Application	Widelands	Widelands	1	All	All	All
Application	Widelands	Widelands	10	All	All	All
Application	Widelands	Widelands	11	All	All	All
Application	Widelands	Widelands	12	All	All	All
Application	Widelands	Widelands	13	All	All	All
Application	Widelands	Widelands	14	All	All	All
Application	Widelands	Widelands	15	All	All	All
Application	Widelands	Widelands	2	All	All	All
Application	Widelands	Widelands	3	All	All	All
Application	Widelands	Widelands	4	All	All	All
Application	Widelands	Widelands	5	All	All	All
Application	Widelands	Widelands	6	All	All	All
Application	Widelands	Widelands	7	All	All	All
Application	Widelands	Widelands	8	All	All	All
Application	Widelands	Widelands	9	All	All	All
Application	Widelands	Widelands	9.5	All	All	All
Application	Widelands	Widelands	All	rc2	All	All
cpe:2.3:a:widelands:widelands:-:build1:*:*:*:*:*:						
cpe:2.3:a:widelands:widelands:-:build10:*:*:*:*:*:						
cpe:2.3:a:widelands:widelands:-:build10_release_candidate:*:*:*:*:*:						
cpe:2.3:a:widelands:widelands:-:build11:*:*:*:*:*:						
cpe:2.3:a:widelands:widelands:-:build11_release_candidate:*:*:*:*:*:						
cpe:2.3:a:widelands:widelands:-:build12:*:*:*:*:*:						
cpe:2.3:a:widelands:widelands:-:build12_release_candidate:*:*:*:*:*:						
cpe:2.3:a:widelands:widelands:-:build13:*:*:*:*:*:						
cpe:2.3:a:widelands:widelands:-:build13_release_candidate:*:*:*:*:*:						

cpe:2.3:a:widelands:widelands:-:build13_release_candidate2:*****:
cpe:2.3:a:widelands:widelands:-:build14:*****:
cpe:2.3:a:widelands:widelands:-:build14_release_candidate:*****:
cpe:2.3:a:widelands:widelands:-:build2:*****:
cpe:2.3:a:widelands:widelands:-:build3:*****:
cpe:2.3:a:widelands:widelands:-:build4:*****:
cpe:2.3:a:widelands:widelands:-:build5:*****:
cpe:2.3:a:widelands:widelands:-:build6:*****:
cpe:2.3:a:widelands:widelands:-:build7:*****:
cpe:2.3:a:widelands:widelands:-:build8:*****:
cpe:2.3:a:widelands:widelands:-:build9:*****:
cpe:2.3:a:widelands:widelands:1:*****:
cpe:2.3:a:widelands:widelands:10:*****:
cpe:2.3:a:widelands:widelands:11:*****:
cpe:2.3:a:widelands:widelands:12:*****:
cpe:2.3:a:widelands:widelands:13:*****:
cpe:2.3:a:widelands:widelands:14:*****:
cpe:2.3:a:widelands:widelands:15:*****:
cpe:2.3:a:widelands:widelands:2:*****:
cpe:2.3:a:widelands:widelands:3:*****:
cpe:2.3:a:widelands:widelands:4:*****:
cpe:2.3:a:widelands:widelands:5:*****:
cpe:2.3:a:widelands:widelands:6:*****:
cpe:2.3:a:widelands:widelands:7:*****:
cpe:2.3:a:widelands:widelands:8:*****:
cpe:2.3:a:widelands:widelands:9:*****:
cpe:2.3:a:widelands:widelands:9.5:*****:
cpe:2.3:a:widelands:widelands:1:*****:
cpe:2.3:a:widelands:widelands:10:*****:

cpe:2.3:a:widelands:widelands:10:*****:
cpe:2.3:a:widelands:widelands:11:*****:
cpe:2.3:a:widelands:widelands:12:*****:
cpe:2.3:a:widelands:widelands:13:*****:
cpe:2.3:a:widelands:widelands:14:*****:
cpe:2.3:a:widelands:widelands:15:*****:
cpe:2.3:a:widelands:widelands:2:*****:
cpe:2.3:a:widelands:widelands:3:*****:
cpe:2.3:a:widelands:widelands:4:*****:
cpe:2.3:a:widelands:widelands:5:*****:
cpe:2.3:a:widelands:widelands:6:*****:
cpe:2.3:a:widelands:widelands:7:*****:
cpe:2.3:a:widelands:widelands:8:*****:
cpe:2.3:a:widelands:widelands:9:*****:
cpe:2.3:a:widelands:widelands:9.5:*****:
cpe:2.3:a:widelands:widelands:*rc2:*****:

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](#)