



CVE-2013-1809

Published on: 11/07/2019 12:00:00 AM UTC

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

CVE-2013-1809

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

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

Gambas before 3.4.0 allows remote attackers to move or manipulate directory contents or perform symlink attacks due to the creation of insecure temporary directories.

CVE-2013-1809 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: gambas3 - gambas3 version = 3.4.0

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **6.4 - MEDIUM**

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

CVE References

Description	Tags	Link
Gambas / Code / Commit [r5438]	Patch Third Party Advisory sourceforge.net	CONFIRM sourceforge.net/p/gambas/code/5438/

	security@openwall.com text/html	
oss-security - Re: CVE Request: Gambas Directory hijack vulnerability	Mailing List Third Party Advisory www.openwall.com text/html	 MISC www.openwall.com/lists/oss-security/2013/03/03/4
CVE-2013-1809	Third Party Advisory security-tracker.debian.org text/html	 MISC security-tracker.debian.org/tracker/CVE-2013-1809
917751 – (CVE-2013-1809) CVE-2013-1809 gambas3: insecure temporary directories flaw	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=CVE-2013-1809
access.redhat.com CVE-2013-1809	Not Applicable Third Party Advisory access.redhat.com text/html	 MISC access.redhat.com/security/cve/cve-2013-1809
Google Code Archive - Long-term storage for Google Code Project Hosting.	Issue Tracking Third Party Advisory code.google.com text/html	 MISC code.google.com/archive/p/gambas/issues/365

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	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gambas Project	Gambas	All	All	All	All
Application	Gambas Project	Gambas	All	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*****:
cpe:2.3:o:debian:debian_linux:10.0:*****:
cpe:2.3:o:debian:debian_linux:8.0:*****:
cpe:2.3:o:debian:debian_linux:9.0:*****:
cpe:2.3:a:gambas_project:gambas:*****:
cpe:2.3:a:gambas_project:gambas:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023 [🐦](#) [N](#) |

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](#)