



CVE-2011-3631

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:19 AM UTC

CVE-2011-3631

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

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

Hardlink before 0.1.2 has multiple integer overflows leading to heap-based buffer overflows because of the way string lengths concatenation is done in the calculation of the required memory space to be used. A remote attacker could provide a specially-crafted directory tree and trick the local user into consolidating it, leading to hardlink executable crash or potentially arbitrary code execution with user privileges.

CVE-2011-3631 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **hardlink** - **hardlink** version = **0.3.0**

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

CVE-2011-3631	Third Party Advisory security-tracker.debian.org text/html	 MISC security-tracker.debian.org/tracker/CVE-2011-3631
CVE-2011-3631 - Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 MISC access.redhat.com/security/cve/cve-2011-3631
#645516 - hardlink: Security issue on changing trees - Debian Bug report logs	Issue Tracking Third Party Advisory bugs.debian.org text/html	 MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=645516
746710 – (CVE-2011-3631) CVE-2011-3631 hardlink: Multiple integer overflows, when adding string lengths	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-3631

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	Hardlink Project	Hardlink	All	All	All	All
Application	Hardlink Project	Hardlink	All	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	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:hardlink_project:hardlink:****:*:*:
cpe:2.3:a:hardlink_project:hardlink:****:*:*:
cpe:2.3:o:redhat:enterprise_linux:5.0:****:*:*:
cpe:2.3:o:redhat:enterprise_linux:6.0:****:*:*:
cpe:2.3:o:redhat:enterprise_linux:5.0:****:*:*:
cpe:2.3:o:redhat:enterprise_linux:6.0:****:*:*:

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