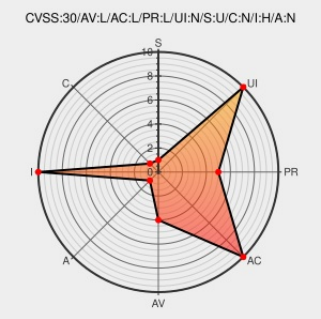
CVE-2011-2684

Published on: 10/23/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:20 PM UTC

CVE-2011-2684

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Foo2zjs from Rkkda contain the following vulnerability:

foo2zjs before 20110722dfsg-3ubuntu1 as packaged in Ubuntu, 20110722dfsg-1 as packaged in Debian unstable, and 20090908dfsg-5.1+squeeze0 as packaged in Debian squeeze create temporary files insecurely, which allows local users to write over arbitrary files via a symlink attack on /tmp/foo2zjs.

CVE-2011-2684 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
#633870 - CVE-2011-2684 - Debian Bug report logs	Third Party Advisory, bugs.debian.org, text/html	MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=633870

Bug #805370 “/usr/bin/getweb is vulnerable to “Insecure temporar...” : Bugs : foo2zjs package : Ubuntu	Third Party Advisory bugs.launchpad.net text/html	MISC bugs.launchpad.net/ubuntu/+source/foo2zjs/+bug/805370
CVE-2011-2684	Third Party Advisory security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2011-2684/
oss-security - Fwd: Old CVE ids, public, but still "RESERVED"	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20140208 Fwd: Old CVE ids, public, but still
oss-security - CVE Request: foo2zjs	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2011/07/06/10

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rkkda	Foo2zjs	20090908dfsg-5.1+squeeze0	All	All	All
Application	Rkkda	Foo2zjs	20090908dfsg-5.1\+squeeze0	All	All	All
Application	Rkkda	Foo2zjs	20110722dfsg-1	All	All	All
Application	Rkkda	Foo2zjs	20110722dfsg-3ubuntu1	All	All	All
Application	Rkkda	Foo2zjs	20090908dfsg-5.1\+squeeze0	All	All	All
Application	Rkkda	Foo2zjs	20110722dfsg-1	All	All	All
Application	Rkkda	Foo2zjs	20110722dfsg-3ubuntu1	All	All	All

cpe:2.3:a:rkkda:foo2zjs:20090908dfsg-5.1+squeeze0:*:*:*:*:*:debian:*:*:

cpe:2.3:a:rkkda:foo2zjs:20090908dfsg-5.1\+squeeze0:*:*:*:*:*:debian:*:*:

cpe:2.3:a:rkkda:foo2zjs:20110722dfsg-1:*:*:*:*:*:debian:*:*:

cpe:2.3:a:rkkda:foo2zjs:20110722dfsg-3ubuntu1:*:*:*:*:*:ubuntu:*:*:

cpe:2.3:a:rkkda:foo2zjs:20090908dfsg-5.1\+squeeze0:*:*:*:*:*:debian:*:*:

cpe:2.3:a:rkkda:foo2zjs:20110722dfsg-1:*:*:*:*:*:debian:*:*:

cpe:2.3:a:rkkda:foo2zjs:20110722dfsg-3ubuntu1:*:*:*:*:*:ubuntu:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→