CVE-2012-5656

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-5656
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-01-18 11:48:00 UTC
Updated	2013-03-23 03:14:00 UTC
Description	The rasterization process in Inkscape before 0.48.4 allows local users to read arbitrary files via an external entity in a SVG f

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Inkscape	Inkscape	0.37	All	All	All
Application	Inkscape	Inkscape	0.38.1	All	All	All
Application	Inkscape	Inkscape	0.39	All	All	All
Application	Inkscape	Inkscape	0.40	All	All	All
Application	Inkscape	Inkscape	0.41	All	All	All
Application	Inkscape	Inkscape	0.42	All	All	All
Application	Inkscape	Inkscape	0.42.2	All	All	All
Application	Inkscape	Inkscape	0.43	All	All	All
Application	Inkscape	Inkscape	0.44	All	All	All
Application	Inkscape	Inkscape	0.44.1	All	All	All
Application	Inkscape	Inkscape	0.45.1	All	All	All
Application	Inkscape	Inkscape	0.46	All	All	All
Application	Inkscape	Inkscape	0.47	All	All	All
Application	Inkscape	Inkscape	0.47	pre0	All	All
Application	Inkscape	Inkscape	0.47	pre1	All	All
Application	Inkscape	Inkscape	0.47	pre2	All	All
Application	Inkscape	Inkscape	0.47	pre3	All	All

Application	Inkscape	Inkscape	0.47	pre4	All	All
Application	Inkscape	Inkscape	0.48	All	All	All
Application	Inkscape	Inkscape	0.48	pre0	All	All
Application	Inkscape	Inkscape	0.48	pre1	All	All
Application	Inkscape	Inkscape	0.48.1	All	All	All
Application	Inkscape	Inkscape	0.48.2	All	All	All
Application	Inkscape	Inkscape	0.48.3	All	All	All
Application	Inkscape	Inkscape	All	All	All	All
Application	Inkscape	Inkscape	0.37	All	All	All
Application	Inkscape	Inkscape	0.38.1	All	All	All
Application	Inkscape	Inkscape	0.39	All	All	All
Application	Inkscape	Inkscape	0.40	All	All	All
Application	Inkscape	Inkscape	0.41	All	All	All
Application	Inkscape	Inkscape	0.42	All	All	All
Application	Inkscape	Inkscape	0.42.2	All	All	All
Application	Inkscape	Inkscape	0.43	All	All	All
Application	Inkscape	Inkscape	0.44	All	All	All
Application	Inkscape	Inkscape	0.44.1	All	All	All
Application	Inkscape	Inkscape	0.45.1	All	All	All
Application	Inkscape	Inkscape	0.46	All	All	All
Application	Inkscape	Inkscape	0.47	All	All	All
Application	Inkscape	Inkscape	0.47	pre0	All	All
Application	Inkscape	Inkscape	0.47	pre1	All	All
Application	Inkscape	Inkscape	0.47	pre2	All	All
Application	Inkscape	Inkscape	0.47	pre3	All	All
Application	Inkscape	Inkscape	0.47	pre4	All	All
Application	Inkscape	Inkscape	0.48	All	All	All
Application	Inkscape	Inkscape	0.48	pre0	All	All
Application	Inkscape	Inkscape	0.48	pre1	All	All
Application	Inkscape	Inkscape	0.48.1	All	All	All
Application	Inkscape	Inkscape	0.48.2	All	All	All
Application	Inkscape	Inkscape	0.48.3	All	All	All

References

Reference	Source	Link
[SECURITY] F... 13 Update to inkscape-0.48.4.1-1.fc13	FEDORA	lists.fedoraproject...

[SECURITY] Fedora 18 Update: inkscape-0.48.4-1.fc18	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 16 Update: inkscape-0.48.4-1.fc16	FEDORA	lists.fedoraproject.org
USN-1712-1: Inkscape vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
0.48.4 : Inkscape	CONFIRM	launchpad.net
Bug #1025185 “XXE vulnerability during rasterization of SVG imag...” : Bugs : Inkscape	CONFIRM	bugs.launchpad.net
~inkscape.dev/inkscape/trunk : revision 11931	CONFIRM	bazaar.launchpad.net
[SECURITY] Fedora 17 Update: inkscape-0.48.4-1.fc17	FEDORA	lists.fedoraproject.org
openSUSE-SU-2013:0294-1: moderate: inkscape: two security fixes	SUSE	lists.opensuse.org
openSUSE-SU-2013:0297-1: moderate: inkscape: two security fixes	SUSE	lists.opensuse.org
504 Gateway Time-out	BID	www.securityfocus.com
oss-security - Re: CVE request: Inkscape fixes a XXE vulnerability during rasterization of SVG images	MLIST	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**