CVE-2008-3522

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

Summary

CVE	CVE-2008-3522
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-02 18:18:00 UTC
Updated	2017-08-08 01:31:00 UTC
Description	Buffer overflow in the jas_stream_printf function in libjasper/base/jas_stream.c in JasPer 1.900.1 might allow context-deper

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jasper Project	Jasper	1.900.1	All	All	All
Application	Jasper Project	Jasper	1.900.1	All	All	All
Application	Redhat	Enterprise Virtualization	3.5	All	All	All
Application	Redhat	Enterprise Virtualization	3.5	All	All	All

References

Reference	Source	Link
JasPer 1.900.1 Multiple Vulnerabilities	BID	www.securityfoc
Support / Security / Advisories / / MDVSA-2009:164 | Mandriva	MANDRIVA	www.mandriva.c
IBM X-Force Exchange	XF	exchange.xforce
Gentoo update for jasper - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Support / Security / Advisories / / MDVSA-2009:142 | Mandriva	MANDRIVA	www.mandriva.c
bugs.gentoo.org/attachment.cgi	MISC	bugs.gentoo.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	www.slackware.
JasPer: User-assisted execution of arbitrary code — Gentoo Linux Documentation	GENTOO	security.gentoo.
Ubuntu update for jasper - Secunia.com	SECUNIA	secunia.com

Support / Security / Advisories / / MDVSA-2009:144 | Mandriva	MANDRIVA	www.mandriva.c
USN-742-1: JasPer vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
Gentoo Bug 222819 - media-libs/jasper <1.900.1-r3 multiple vulnerabilities (CVE-2008-{3520,3521,3522})	MISC	bugs.gentoo.org
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**