



CVE-2010-4262

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2010-4262
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-17 19:00:00 UTC
Updated	2011-01-20 06:46:00 UTC
Description	Stack-based buffer overflow in Xfig 3.2.4 and 3.2.5 allows remote attackers to cause a denial of service (crash) and possibl

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xfig	Xfig	3.2.4	All	All	All
Application	Xfig	Xfig	3.2.5	All	All	All
Application	Xfig	Xfig	3.2.4	All	All	All
Application	Xfig	Xfig	3.2.5	All	All	All

References

Reference	Source	Link
Xfig '.fig' File Color Definition Stack Buffer Overflow Vulnerability	BID	www.bidsa.org
oss-security - CVE Request -- Xfig: Stack-based buffer overflow by processing FIG image with crafted color definition	MLIST	www.oss-security.com
Support / Security / Advisories / / MDVSA-2011:010 Mandriva	MANDRIVA	www.mandriva.com
Fedora update for xfig - Advisories - Community	SECUNIA	secunia.com
[SECURITY] Fedora 14 Update: xfig-3.2.5-25.b.fc14	FEDORA	lists.fedoraproject.org
659676 -- (CVE-2010-4262) CVE-2010-4262 Xfig: Stack-based buffer overflow by processing certain FIG images	CONFIRM	bugzilla.redhat.com
oss-security - Re: CVE Request -- Xfig: Stack-based buffer overflow by processing FIG image with crafted color definition	MLIST	www.oss-security.com
Webmail - OVH	VUPEN	www.vupen.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
657981 -- xfig buffer overflow when opening .fig file with malicious colour definition	MISC	bugzilla.redhat.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.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)