



CVE-2013-3934

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2013-3934
State	PUBLIC
Assigner	PSIRT-CNA@flexerasoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-09-10 19:55:00 UTC
Updated	2013-09-10 23:05:00 UTC
Description	Stack-based buffer overflow in Kingsoft Writer 2012 8.1.0.3030, as used in Kingsoft Office 2013 before 9.1.0.4256, allows r

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kingsoft	Office 2012	8.1.0.3385	All	All	All
Application	Kingsoft	Office 2012	8.1.0.3385	All	All	All
Application	Kingsoft	Writer 2012	8.1.0.3030	All	All	All
Application	Kingsoft	Writer 2012	8.1.0.3030	All	All	All

References

Reference	Source	Link
Security Advisory SA53266 - Kingsoft Writer 2012 WPS Font Names Buffer Overflow Vulnerability - Secunia	SECUNIA	secunia.com
Kingsoft Writer CVE-2013-3934 Stack Buffer Overflow Vulnerability	BID	www.securityfo
Kingsoft Writer Buffer Overflow Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.securitytra
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](#).

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