



CVE-2014-9527

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

Summary

CVE	CVE-2014-9527
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-06 15:59:00 UTC
Updated	2017-02-11 02:59:00 UTC
Description	HSLFSlideShow in Apache POI before 3.11 allows remote attackers to cause a denial of service (infinite loop and deadlock

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Poi	All	beta3	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	access.redhat.com
[SECURITY] Fedora 20 Update: apache-poi-3.10.1-2.fc20	FEDORA	lists.fedoraproject.org
History of Changes	CONFIRM	poi.apache.org
Security Advisory SA61953 - Apache POI PPT File Parsing Denial of Service Vulnerability - Secunia	SECUNIA	secunia.com
Bug 57272 – [PATCH]: Deadlock on corrupted PPT file	CONFIRM	issues.apache.org
POI CVE-2014-9527 Denial-Of-Service Vulnerability	BID	www.securityfocus.com
Security Bulletin: Vulnerabilities in Apache POI affects IBM InfoSphere Information Server	CONFIRM	www-01.ibm.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](#).

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