



# CVE-2010-2936

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

## Summary

<b>CVE</b>	CVE-2010-2936
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-08-25 20:00:00 UTC
<b>Updated</b>	2023-02-13 03:19:00 UTC
<b>Description</b>	Integer overflow in simpres.bin in the Impress module in OpenOffice.org (OOo) 2.x and 3.x before 3.3 allows remote attack

## Risk And Classification

**Problem Types:** CWE-189

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Application	Openoffice	Openoffice.org	3.2.1	All	All	All
Application	Openoffice	Openoffice.org	3.2.1	All	All	All

## References

Reference	Source
Webmail - OVH	VULNERABILITY
OpenOffice.org Mailing List Archives	MISC
Oracle Critical Patch Update Pre-Release Announcement - January 2011	CVE
OpenOffice.org Multiple Vulnerabilities - Advisories - Community	SECURITY
Advisories   Mandriva	MISC
Debian update for openoffice.org - Advisories - Community	SECURITY
Bug 622555 – CVE-2010-2936 OpenOffice.org: Heap-based buffer overflow by parsing specially-crafted Microsoft PowerPoint document	CVE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VULNERABILITY
Security Advisory SA60799 - Gentoo openoffice Multiple Vulnerabilities - Secunia	SECURITY
Red Hat update for openoffice.org - Advisories - Community	SECURITY

Oracle Open Office Two Vulnerabilities - Advisories - Community	SE
Ubuntu update for openoffice.org - Advisories - Community	SE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VL
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:024	SU
CVE-2010-2935	CO
OpenOffice Bugs in Processing PowerPoint Files Let Remote Users Execute Arbitrary Code - SecurityTracker	SE
Repository / Oval Repository	O'
USN-1056-1: OpenOffice.org vulnerabilities   Ubuntu	UF
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VL
Red Hat Customer Portal	MI
Gentoo Linux Documentation -- OpenOffice, LibreOffice: Multiple vulnerabilities	GI
oss-security - Re: CVE Request -- OpenOffice.org [two ids]: 1, integer truncation error 2, short integer overflow	MI
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:019	SU
Debian -- Security Information -- DSA-2099-1 openoffice.org	DI
oss-security - CVE Request -- OpenOffice.org [two ids]: 1, integer truncation error 2, short integer overflow	MI
Webmail - OVH	VL
SecurityTracker.com Archives - OpenOffice.org Impress Buffer Overflows Let Remote Users Execute Arbitrary Code	SE
access.redhat.com   CVE-2010-2936	MI
rhn.redhat.com   Red Hat Support	RF
Bug 622529 – CVE-2010-2935 OpenOffice.Org: Integer truncation error by parsing specially-crafted Microsoft PowerPoint document	CO
securityevaluators.com/files/papers/CrashAnalysis.pdf	MI
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VL
CVE Program record	CV
NVD vulnerability detail	NV

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](#).

