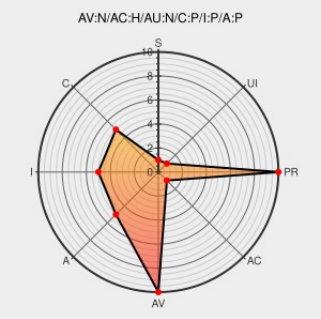
CVE-2005-0941

Published on: 04/12/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:26 PM UTC

CVE-2005-0941

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openoffice from Openoffice contain the following vulnerability:

The StgCompObjStream::Load function in OpenOffice.org OpenOffice 1.1.4 and earlier allocates memory based on 16 bit length values, but process memory using 32 bit values, which allows remote attackers to cause a denial of service and possibly execute arbitrary code via a DOC document with certain length values, which leads to a heap-based buffer overflow.

CVE-2005-0941 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.1 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2005:021
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20050412 OpenOffice DOC document Heap Overflow
Gentoo Linux Documentation -- OpenOffice.Org: DOC document Heap Overflow	www.gentoo.org text/html	GENTOO GLSA-200504-13
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9106
OpenOffice Malformed Document Remote Heap Overflow	cve.report (archive)	BID 13092

Vulnerability	text/html	
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:375
Search by bug number	www.openoffice.org text/html	CONFIRM www.openoffice.org/issues/show_bug.cgi?id=46388
Secunia - Advisories - SUSE Updates for Multiple Packages	web.archive.org text/html	SECUNIA 17027

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openoffice	Openoffice	1.0.1	All	All	All
Application	Openoffice	Openoffice	1.0.2	All	All	All
Application	Openoffice	Openoffice	1.1.0	All	All	All
Application	Openoffice	Openoffice	1.1.1	All	All	All
Application	Openoffice	Openoffice	1.1.2	All	All	All
Application	Openoffice	Openoffice	1.1.3	All	All	All
Application	Openoffice	Openoffice	1.1.4	All	All	All
Application	Openoffice	Openoffice	1.0.1	All	All	All
Application	Openoffice	Openoffice	1.0.2	All	All	All
Application	Openoffice	Openoffice	1.1.0	All	All	All
Application	Openoffice	Openoffice	1.1.1	All	All	All
Application	Openoffice	Openoffice	1.1.2	All	All	All
Application	Openoffice	Openoffice	1.1.3	All	All	All
Application	Openoffice	Openoffice	1.1.4	All	All	All

cpe:2.3:a:openoffice:openoffice:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:openoffice:openoffice:1.1.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→