



CVE-2007-2895

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

Summary

CVE	CVE-2007-2895
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-30 01:30:00 UTC
Updated	2017-07-29 01:31:00 UTC
Description	Buffer overflow in a certain ActiveX control in LTRDF14e.DLL 14.5.0.44 in LeadTools Raster Dialog File Object allows remote attackers to execute arbitrary code or cause a denial of service (crash) by sending a crafted request to the application. The vulnerability exists because the application does not properly validate the length of the data received from the remote attacker, which can lead to a buffer overflow. This vulnerability affects LeadTools Raster Dialog File Object 14.5.0.44 and earlier. The vulnerability is caused by a buffer overflow in the LTRDF14e.DLL ActiveX control. The vulnerability is caused by a buffer overflow in the LTRDF14e.DLL ActiveX control. The vulnerability is caused by a buffer overflow in the LTRDF14e.DLL ActiveX control.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lead Technologies	Leadtools Raster Dialog File Object	14.5.0.44	All	All	All
Application	Lead Technologies	Leadtools Raster Dialog File Object	14.5.0.44	All	All	All

References

Reference

IBM X-Force Exchange
LEADTOOLS LEAD Raster Dialog File Object ActiveX Control Memory Corruption - Advisories - Secunia
shinnai.altervista.org
LeadTools Raster Dialog File Object LTRDF14E.DLL ActiveX Control Buffer Overflow Vulnerability
36035
shinnai.altervista.org
MoAxB - Month of ActiveX Bug: MoAxB #24: LeadTools Raster Dialog File Object (LTRDF14e.DLL v. 14.5.0.44) Remote Buffer Overflow Exploit
CVE Program record
NVD vulnerability detail

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](#)