



CVE-2006-2391

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2006-2391
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-05-16 01:02:00 UTC
Updated	2018-10-18 16:39:00 UTC
Description	Buffer overflow in EMC Retrospect Client 5.1 through 7.5 allows remote attackers to cause a denial of service (crash) and p

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Retrospect Client	5.1	All	All	All
Application	Emc	Retrospect Client	6.5	All	All	All
Application	Emc	Retrospect Client	7.0	All	All	All
Application	Emc	Retrospect Client	7.5	All	All	All
Application	Emc	Retrospect Client	5.1	All	All	All
Application	Emc	Retrospect Client	6.5	All	All	All
Application	Emc	Retrospect Client	7.0	All	All	All
Application	Emc	Retrospect Client	7.5	All	All	All

References

Reference	Source	Link
EMC Retrospect Client Buffer Overflow Vulnerability	BID	www.securityfocus.com
Webmail - OVH	VUPEN	www.vupen.com
www.acrossecurity.com/aspr/ASPR-2006-05-17-1-PUB.txt	MISC	www.acrossecurity.com
About Secunia Research Flexera	SECUNIA	secunia.com
EMC Retrospect Client Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	securitytracker.com
EMC Retrospect Client Buffer Overflow Lets Remote Users Deny Service - SecurityTracker	SECTRACK	securitytracker.com

IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
EMC Dantz Retrospect Backup Client Remote Buffer Overflow Vulnerability	BID	www.securityfocus.com
kb.dantz.com/display/2n/articleDirect/index.asp	CONFIRM	kb.dantz.com
US-CERT Vulnerability Note VU#186944	CERT-VN	www.kb.cert.org
SecurityFocus	BUGTRAQ	www.securityfocus.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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report