



CVE-2007-5323

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

Summary

CVE	CVE-2007-5323
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-11 00:17:00 UTC
Updated	2017-07-29 01:33:00 UTC
Description	The RepliStor Server Service in EMC Replistor 6.1.3 allows remote attackers to execute arbitrary code via a size value that

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Replistor	6.1.3	All	All	All
Application	Emc	Replistor	6.1.3	All	All	All

References

Reference	Source	Link
EMC RepliStor Server Service Buffer Overflow Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xforce
SecurityTracker.com Archives - EMC RepliStor Buffer Overflow Lets Remote Users Execute Arbitrary Code	SECTrack	www.securitytrac
EMC RepliStor Server Service recv() Buffer Overflow Vulnerability	BID	www.securityfocu
TippingPoint DVLabs	MISC	dvlabs.tippingpoi
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.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](#).

Free CVE JSON API [cve.report/api](#)

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