



CVE-2007-3618

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

Summary

CVE	CVE-2007-3618
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-08-21 21:17:00 UTC
Updated	2018-10-15 21:29:00 UTC
Description	Stack-based buffer overflow in the NetWorker Remote Exec Service (nsrexecd.exe) in EMC Software NetWorker 7.x.x allow

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Legato Networker	7.0	All	All	All
Application	Emc	Legato Networker	7.1.3	All	All	All
Application	Emc	Legato Networker	7.2	All	All	All
Application	Emc	Legato Networker	7.2.1	All	All	All
Application	Emc	Legato Networker	7.3.2	All	All	All
Application	Emc	Legato Networker	7.0	All	All	All
Application	Emc	Legato Networker	7.1.3	All	All	All
Application	Emc	Legato Networker	7.2	All	All	All
Application	Emc	Legato Networker	7.2.1	All	All	All
Application	Emc	Legato Networker	7.3.2	All	All	All

References

Reference	Source
SecurityFocus	BUGTRAQ
ZDI-07-049	MISC
EMC NetWorker Remote Exec Service Buffer Overflow - Advisories - Secunia	SECUNIA
SecurityTracker.com Archives - EMC Legato NetWorker 'subcmd' Stack Overflow Lets Remote Users Execute Arbitrary Code	SECTRACK

39744	OSVDB
EMC Legato Networker Remote Exec Service Stack Overflow Vulnerabilities - CXSecurity.com	SREASON
IBM X-Force Exchange	XF
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
EMC Legato Networker Remote Exec Service Stack Buffer Overflow Vulnerability	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



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](#)