



CVE-2010-1919

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

Summary

CVE	CVE-2010-1919
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-05-28 18:30:00 UTC
Updated	2014-05-05 04:43:00 UTC
Description	Unspecified vulnerability in EMC Avamar 4.1.x and 5.0 before SP1 allows remote attackers to cause a denial of service (gs

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Avamar	4.1	All	All	All
Application	Emc	Avamar	4.1	All	All	All
Application	Emc	Avamar	All	All	All	All

References

Reference	Source	Link
Files ≈ Packet Storm	MISC	www.pack
20100526 ESA-2010-007: EMC Avamar Denial Of Service Vulnerability	BUGTRAQ	archives.n
EMC Avamar TCP Packet Processing Denial of Service - Secunia.com	SECUNIA	secunia.cc
SecurityTracker.com Archives - EMC Avamar Unspecified Flaw in gsan Service Lets Remote Users Deny Service	SECTRACK	securitytra
EMC Avamar 'gsan' Service Denial of Service Vulnerability	BID	www.secu
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupe
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

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](#).

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