



CVE-2007-6689

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

Summary

CVE	CVE-2007-6689
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-17 02:00:00 UTC
Updated	2008-11-15 07:06:00 UTC
Description	Menalto Gallery before 2.2.4 does not properly check for malicious file extensions during file uploads, which allows attacker

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Menalto	Gallery	All	All	All	All

References

Reference	Source
Gentoo Bug 203217 - www-apps/gallery < 2.2.4 Multiple vulnerabilities (CVE-2007-{6685,6686,6687,6688,6689,6690,6691,6692,6693})	CO
Gentoo update for gallery - Advisories - Secunia	SE
Gentoo Linux Documentation -- Gallery: Multiple vulnerabilities	GE
Gallery 2.2.4 Security Fix Release Gallery	CO
41669	OS
CVE Program record	CV
NVD vulnerability detail	NV

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](#)