CVE-2008-4129

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-4129
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-18 20:00:00 UTC
Updated	2017-08-08 01:32:00 UTC
Description	Gallery before 1.5.9, and 2.x before 2.2.6, does not properly handle ZIP archives containing symbolic links, which allows re

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gallery	Gallery	2.2.0	All	All	All
Application	Gallery	Gallery	2.2.1	All	All	All
Application	Gallery	Gallery	2.2.2	All	All	All
Application	Gallery	Gallery	2.2.3	All	All	All
Application	Gallery	Gallery	2.2.4	All	All	All
Application	Gallery	Gallery	2.2.0	All	All	All
Application	Gallery	Gallery	2.2.1	All	All	All
Application	Gallery	Gallery	2.2.2	All	All	All
Application	Gallery	Gallery	2.2.3	All	All	All
Application	Gallery	Gallery	2.2.4	All	All	All
Application	Gallery	Gallery	All	All	All	All
Application	Gallery	Gallery	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 9 Update: gallery2-2.3-1.fc9	FEDORA	www.redhat
Gallery 1.5.9 Released | Gallery	CONFIRM	gallery.men

Gallery Prior to 2.2.6 Multiple Vulnerabilities	BID	www.securi
[SECURITY] Fedora 8 Update: gallery2-2.3-1.fc8	FEDORA	www.redhat
Security Advisory SA32662 - Gentoo update for gallery - Secunia	SECUNIA	secunia.com
Fedora update for gallery2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Gallery 2.2.6 Security Fix Release | Gallery	CONFIRM	gallery.men
Gentoo Linux Documentation -- Gallery: Multiple vulnerabilities	GENTOO	security.ger
Gallery Symlink ZIP Archive Information Disclosure - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.x
CVE Program record	CVE.ORG	www.cve.or
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.

Free CVE JSON API cve.report/api

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