



CVE-2004-0522

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

Summary

CVE	CVE-2004-0522
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-06 04:00:00 UTC
Updated	2017-07-11 01:30:00 UTC
Description	Gallery 1.4.3 and earlier allows remote attackers to bypass authentication and obtain Gallery administrator privileges.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	3.0	All	All	All
Operating System	Debian	Debian Linux	3.0	All	alpha	All
Operating System	Debian	Debian Linux	3.0	All	arm	All
Operating System	Debian	Debian Linux	3.0	All	hppa	All
Operating System	Debian	Debian Linux	3.0	All	ia-32	All
Operating System	Debian	Debian Linux	3.0	All	ia-64	All
Operating System	Debian	Debian Linux	3.0	All	m68k	All
Operating System	Debian	Debian Linux	3.0	All	mips	All
Operating System	Debian	Debian Linux	3.0	All	mipsel	All
Operating System	Debian	Debian Linux	3.0	All	ppc	All
Operating System	Debian	Debian Linux	3.0	All	s-390	All
Operating System	Debian	Debian Linux	3.0	All	sparc	All
Operating System	Debian	Debian Linux	3.0	All	All	All
Operating System	Debian	Debian Linux	3.0	All	alpha	All
Operating System	Debian	Debian Linux	3.0	All	arm	All
Operating System	Debian	Debian Linux	3.0	All	hppa	All
Operating System	Debian	Debian Linux	3.0	All	ia-32	All

Operating System	Debian	Debian Linux	3.0	All	ia-64	All
Operating System	Debian	Debian Linux	3.0	All	m68k	All
Operating System	Debian	Debian Linux	3.0	All	mips	All
Operating System	Debian	Debian Linux	3.0	All	mipsel	All
Operating System	Debian	Debian Linux	3.0	All	ppc	All
Operating System	Debian	Debian Linux	3.0	All	s-390	All
Operating System	Debian	Debian Linux	3.0	All	sparc	All
Application	Gallery Project	Gallery	1.4	All	All	All
Application	Gallery Project	Gallery	1.4.1	All	All	All
Application	Gallery Project	Gallery	1.4.2	All	All	All
Application	Gallery Project	Gallery	1.4.3_pl1	All	All	All
Application	Gallery Project	Gallery	1.4_pl1	All	All	All
Application	Gallery Project	Gallery	1.4_pl2	All	All	All
Application	Gallery Project	Gallery	1.4	All	All	All
Application	Gallery Project	Gallery	1.4.1	All	All	All
Application	Gallery Project	Gallery	1.4.2	All	All	All
Application	Gallery Project	Gallery	1.4.3_pl1	All	All	All
Application	Gallery Project	Gallery	1.4_pl1	All	All	All
Application	Gallery Project	Gallery	1.4_pl2	All	All	All

References			
Reference	Source	Link	Tags
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Debian -- Security Information -- DSA-512-1 gallery	DEBIAN	www.debian.org	Patch, Vendor Advi
Gallery Authentication Bypass Vulnerability	BID	www.securityfocus.com	Patch, Vendor Advi
Secunia - Advisories - Gallery User Authentication Bypass Vulnerability	SECUNIA	secunia.com	
Gentoo Linux Documentation -- Gallery: Privilege escalation vulnerability	GENTOO	security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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