



CVE-2011-2691

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

Summary

CVE	CVE-2011-2691
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-07-17 20:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The png_err function in pngerror.c in libpng 1.0.x before 1.0.55, 1.2.x before 1.2.45, 1.4.x before 1.4.8, and 1.5.x before 1.5.16 has a buffer overflow that can be exploited to crash the application or execute arbitrary code.

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Problem Types: CWE-476 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:M/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libpng	Libpng	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Bug 720608 – CVE-2011-2691 libpng: Crash in png_default_error due to use of NULL Pointer	af854a3a-2127-422b-b000-000000000000
Security Alerts - Secunia	af854a3a-2127-422b-b000-000000000000
oss-security - Security issues fixed in libpng 1.5.4	af854a3a-2127-422b-b000-000000000000
Security Alerts - Secunia	af854a3a-2127-422b-b000-000000000000
LIBPNG: PNG reference library / Git tools	af854a3a-2127-422b-b000-000000000000
[SECURITY] Fedora 14 Update: libpng-1.2.46-1.fc14	af854a3a-2127-422b-b000-000000000000
APPLE-SA-2011-10-12-3 OS X Lion v10.7.2 and Security Update 2011-006	af854a3a-2127-422b-b000-000000000000
libpng Multiple Vulnerabilities - Secunia.com	af854a3a-2127-422b-b000-000000000000
Gentoo Linux Documentation -- libpng: Multiple vulnerabilities	af854a3a-2127-422b-b000-000000000000
Debian -- Security Information -- DSA-2287-1 libpng	af854a3a-2127-422b-b000-000000000000

About the security content of OS X Lion v10.7.2 and Security Update 2011-006	af854a3a-2127-422t
'[security bulletin] HPSBMU02776 SSRT100852 rev.1 - HP Onboard Administrator (OA), Remote Unauthorized' - MARC	af854a3a-2127-422t
Security Alerts - Secunia	af854a3a-2127-422t
libpng Buffer Overflow and Denial of Service Vulnerabilities	af854a3a-2127-422t
IBM X-Force Exchange	af854a3a-2127-422t
libpng Home Page	af854a3a-2127-422t
Support / Security / Advisories // MDVSA-2011:151 Mandriva	af854a3a-2127-422t
LIBPNG: PNG reference library / Git tools	MITRE
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](#)