CVE-2013-6954

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

Summary

CVE	CVE-2013-6954
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-12 18:34:00 UTC
Updated	2018-01-05 02:29:00 UTC
Description	The png_do_expand_palette function in libpng before 1.6.8 allows remote attackers to cause a denial of service (NULL poir

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libpng	Libpng	1.6.0	All	All	All
Application	Libpng	Libpng	1.6.0	beta	All	All
Application	Libpng	Libpng	1.6.1	All	All	All
Application	Libpng	Libpng	1.6.1	beta	All	All
Application	Libpng	Libpng	1.6.2	All	All	All
Application	Libpng	Libpng	1.6.2	beta	All	All
Application	Libpng	Libpng	1.6.3	All	All	All
Application	Libpng	Libpng	1.6.3	beta	All	All
Application	Libpng	Libpng	1.6.4	All	All	All
Application	Libpng	Libpng	1.6.4	beta	All	All
Application	Libpng	Libpng	1.6.5	All	All	All
Application	Libpng	Libpng	1.6.6	All	All	All
Application	Libpng	Libpng	1.6.7	All	All	All
Application	Libpng	Libpng	1.6.7	beta	All	All
Application	Libpng	Libpng	1.6.0	All	All	All
Application	Libpng	Libpng	1.6.0	beta	All	All
Application	Libpng	Libpng	1.6.1	All	All	All

Application	Libpng	Libpng	1.6.1	beta	All	All
Application	Libpng	Libpng	1.6.2	All	All	All
Application	Libpng	Libpng	1.6.2	beta	All	All
Application	Libpng	Libpng	1.6.3	All	All	All
Application	Libpng	Libpng	1.6.3	beta	All	All
Application	Libpng	Libpng	1.6.4	All	All	All
Application	Libpng	Libpng	1.6.4	beta	All	All
Application	Libpng	Libpng	1.6.5	All	All	All
Application	Libpng	Libpng	1.6.6	All	All	All
Application	Libpng	Libpng	1.6.7	All	All	All
Application	Libpng	Libpng	1.6.7	beta	All	All
Application	Libpng	Libpng	All	beta	All	All

References

Reference
libpng Home Page
'[security bulletin] HPSBUX03092 SSRT101668 rev.1 - HP-UX running Java6, Remote Unauthorized Access, ' - MARC
Red Hat Customer Portal
Support / Security / Advisories / / MDVSA-2014:035 | Mandriva
IBM Security Bulletin: Multiple vulnerabilities in IBM SDK for Java included with IBM Forms Viewer - United States
IBM Security Bulletin: InfoSphere Streams is possibly affected by vulnerabilities in the IBM® SDK, Java™ Technology Edition (CVE-2014-045
openSUSE-SU-2014:0100-1: moderate: update for libpng16
libpng 'png_read_transform_info()' Function NULL Pointer Dereference Denial of Service Vulnerability
LIBPNG: PNG reference library - Browse Files at SourceForge.net
Bug 1045561 – CVE-2013-6954 libpng: unhandled zero-length PLTE chunk or NULL palette
Oracle Critical Patch Update - April 2014
Security Advisory SA59058 - IBM Lotus Expeditor Multiple Java Vulnerabilities - Secunia
[SECURITY] Fedora 20 Update: libpng12-1.2.50-6.fc20
Mageia Advisory: MGASA-2014-0075 - Updated libpng and libpng12 packages fix security vulnerability
Security Advisory SA58974 - IBM Forms Viewer Multiple Java Vulnerabilities - Secunia
'[security bulletin] HPSBUX03091 SSRT101667 rev.1 - HP-UX running Java7, Remote Unauthorized Access, ' - MARC
Red Hat Customer Portal
Gentoo Linux Documentation -- IcedTea JDK: Multiple vulnerabilities
LIBPNG: PNG reference library / Code / Commit [1faa6f]
Vulnerability Note VU#650142 - libpng 1.6.1 through 1.6.7 contain a null-pointer dereference vulnerability

[SECURITY] Fedora 20 Update: libpng15-1.5.17-2.fc20
[SECURITY] Fedora 19 Update: libpng12-1.2.50-4.fc19
[SECURITY] Fedora 19 Update: libpng10-1.0.60-6.fc19
[SECURITY] Fedora 20 Update: libpng10-1.0.60-6.fc20
IBM Security Bulletin: IBM Lotus Expeditor fixes for multiple vulnerabilities in IBM JRE - United States
CVE Program record
NVD vulnerability detail

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 registred 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**