



CVE-2010-1205

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

Summary

CVE	CVE-2010-1205
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-30 18:30:00 UTC
Updated	2023-11-07 02:05:00 UTC
Description	Buffer overflow in pngpread.c in libpng before 1.2.44 and 1.4.x before 1.4.3, as used in progressive applications, might allow

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All
Application	Apple	Itunes	All	All	All	All
Application	Apple	Itunes	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X Server	All	All	All	All
Operating System	Apple	Mac Os X Server	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Apple	Safari	All	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All

Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Fedoraproject	Fedora	12	All	All	All
Operating System	Fedoraproject	Fedora	13	All	All	All
Operating System	Fedoraproject	Fedora	12	All	All	All
Operating System	Fedoraproject	Fedora	13	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Libpng	Libpng	All	All	All	All
Application	Libpng	Libpng	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
Application	Vmware	Player	All	All	All	All
Application	Vmware	Player	All	All	All	All
Application	Vmware	Workstation	All	All	All	All
Application	Vmware	Workstation	All	All	All	All

References
Reference
[SECURITY] Fedora 12 Update: libpng10-1.0.54-1.fc12
About the security content of Safari 5.0.4
APPLE-SA-2010-11-10-1 Mac OS X v10.6.5 and Security Update 2010-007
570451 – (CVE-2010-1205) segmentation fault when viewing a malformed PNG image
Ubuntu update for libpng - Advisories - Community
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
SourceForge - libpng/libpng/commitdiff
Debian -- Security Information -- DSA-2072-1 libpng
libpng Home Page
Apple iOS Multiple Vulnerabilities - Advisories - Community
KB27244-Vulnerabilities in BlackBerry Enterprise Server components that process images could allow remote code execution
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:017
About the security content of iTunes 10.2 - Apple Support
SourceForge - libpng/libpng/commitdiff
IBM X-Force Exchange
libpng Memory Corruption and Memory Leak Vulnerabilities
Debian update for libpng - Advisories - Community
APPLE-SA-2011-03-09-2 Safari 5.0.4
libpng Two Vulnerabilities - Advisories - Community
About the security content of Apple TV software update 4.1
Google Chrome Releases: Stable Channel Update
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
[SECURITY] Fedora 13 Update: libpng10-1.0.54-1.fc13
Webmail - OVH
Repository / Oval Repository
APPLE-SA-2010-08-24-1 Security Update 2010-005
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
The Slackware Linux Project: Slackware Security Advisories
USN-960-1: libpng vulnerabilities Ubuntu
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
MFSA 2010-41: Remote code execution using malformed PNG image
Support / Security / Advisories // MDVSA-2010:133 Mandriva
Issue 45983 - chromium - Segmentation fault in WebCore::RenderLayer::paintList when a malformed PNG image is viewed - Project Hosting c
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Apple TV Multiple Vulnerabilities - Advisories - Community
VMSA-2010-0014
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
VMware Update for Workstation and Player - Advisories - Community
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
APPLE-SA-2011-03-02-1 iTunes 10.2
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Changeset 61816 – WebKit
About the security content of iOS 4.2
APPLE-SA-2010-11-22-1 iOS 4.2
Access Denied
Bug 608238 – CVE-2010-1205 libpng: out-of-bounds memory write
About Security Update 2010-005
[Security-announce] VMSA-2010-0014 VMware Workstation, Player, and ACE address several security issues
About the security content of Mac OS X v10.6.5 and Security Update 2010-007
Slackware update for libpng - Advisories - Community
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.