



CVE-2007-6352

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

Summary

CVE	CVE-2007-6352
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-20 02:46:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Integer overflow in libexif 0.6.16 and earlier allows context-dependent attackers to execute arbitrary code via an image with

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				
[SECURITY] Fedora 7 Update: libexif-0.6.15-3.fc7				
Security Announcement				
libexif Image Tag Remote Integer Overflow Vulnerability				
Ubuntu update for libexif - Secunia Advisories - Vulnerability Intelligence - Secunia.com				
Repository / Oval Repository				
Bug 425561 – CVE-2007-6352 libexif integer overflow				
Bug 425631 – CVE-2007-6351 CVE-2007-6352 libexif various flaws [F8]				
Gentoo Bug 202350 - media-libs/libexif < 0.6.16-r1 Multiple vulnerabilities (CVE-2007-{6351,6352})				
Mandriva update for libexif - Secunia Advisories - Vulnerability Intelligence - Secunia.com				
SecurityFocus				
IBM X-Force Exchange				
Gentoo update for libexif - Secunia Advisories - Vulnerability Intelligence - Secunia.com				
Debian update for libexif - Advisories - Secunia				
libexif Integer Overflow and Denial of Service - Advisories - Secunia				
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				
rhn.redhat.com Red Hat Support				
Gentoo Linux Documentation -- libexif: Multiple vulnerabilities				
Repository / Oval Repository				
rhn.redhat.com Red Hat Support				
Sun Solaris libexif Integer Overflow Vulnerability - Advisories - Secunia				
osvdb.org/42653				
USN-654-1: libexif vulnerabilities Ubuntu				
Red Hat update for libexif - Advisories - Secunia				
[SECURITY] Fedora 8 Update: libexif-0.6.15-5.fc8				
rPath update for libexif - Advisories - Secunia				
libexif Infinite Recursion Bug Permits Denial of Service Attacks and Integer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTra				
issues.rpath.com/browse/RPL-2068				
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com				
Debian -- Security Information -- DSA-1487-1 libexif				
Security Advisories Mandriva Linux				

Security Advisories Mandriva Linux
Bug 425621 – CVE-2007-6351 CVE-2007-6352 libexif various flaws [F7]
Webmail- OVH
Fedora update for libexif - Advisories - Secunia
sunsolve.sun.com/search/document.do
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 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