



CVE-2005-1849

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2005-1849 |
| State | PUBLIC |
| Assigner | security@debian.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2005-07-26 04:00:00 UTC |
| Updated | 2022-06-22 16:40:00 UTC |
| Description | infrees.h in zlib 1.2.2 allows remote attackers to cause a denial of service (application crash) via an invalid file that causes |

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------------------|----------------------|---------|--------|---------|----------|
| Application | Gnu | Zlib | 1.2.2 | All | All | All |
| Application | Gnu | Zlib | 1.2.2 | All | All | All |
| Application | Zlib | Zlib | 1.2.2 | All | All | All |

References

| Reference | Source | Link |
|--|----------|--|
| 18141 | OSVDB | www.osvdb.org |
| SecurityFocus | BUGTRAQ | www.securityfocus.com |
| Support | REDHAT | www.redhat.com |
| Secunia - Advisories - SCO OpenServer update for zlib | SECUNIA | secunia.com |
| USN-151-3: zlib vulnerabilities Ubuntu security notices Ubuntu | UBUNTU | www.ubuntulinux.org |
| Secunia - Advisories - Ubuntu update for lsb-rpm | SECUNIA | secunia.com |
| Gentoo Linux Documentation -- Qt: Buffer overflow in the included zlib library | GENTOO | www.gentoo.org |
| Advisories - Mandriva Linux OS | MANDRIVA | www.mandriva.com |
| 162680 – CAN-2005-2096 zlib buffer overflow | FEDORA | bugzilla.redhat.com |
| Secunia - Advisories - zlib Denial of Service Vulnerability | SECUNIA | secunia.com |
| Support | REDHAT | www.redhat.com |

| | | |
|--|----------|--|
| Zlib Compression Library Decompression Buffer Overflow Vulnerability | BID | www.securityfocus.com |
| Advisories - Mandriva Linux OS | MANDRIVA | www.mandriva.com |
| Debian -- Security Information -- DSA-1026-1 sash | DEBIAN | www.debian.org |
| IBM X-Force Exchange | XF | exchange.xforce.ibmcloud.com |
| Secunia - Advisories - Mandriva update for perl-Compress-Zlib | SECUNIA | secunia.com |
| Repository / Oval Repository | OVAL | oval.cisecurity.org |
| Download Patch ESX-3616065 for VMware ESX Server 3.0.0 | CONFIRM | www.vmware.com |
| Download Patch ESX-9916286 for VMware ESX Server 3.0.1 | CONFIRM | www.vmware.com |
| Gentoo Linux Documentation -- Pngcrush: Buffer overflow | GENTOO | www.gentoo.org |
| Gentoo update for pngcrush - Advisories - Secunia | SECUNIA | secunia.com |
| VMware ESX Server Multiple Vulnerabilities - Advisories - Secunia | SECUNIA | secunia.com |
| 404 Not Found | MISC | security.debian.org |
| Debian update for sash - Advisories - Secunia | SECUNIA | secunia.com |
| Debian -- Security Information -- DSA-797-2 zsync | DEBIAN | www.debian.org |
| Security Announcement | SUSE | www.novell.com |
| Secunia - Advisories - Mandriva update for sash | SECUNIA | secunia.com |
| Red Hat Network Satellite Server Update for Solaris Client - Advisories - Community | SECUNIA | secunia.com |
| APPLE-SA-2005-08-17 Security Update 2005-007 v1.1 | APPLE | lists.apple.com |
| APPLE-SA-2005-08-15 Security Update 2005-007 | APPLE | lists.apple.com |
| SecurityTracker.com Archives - zlib Buffer Overflow in 'inftrees.c' Lets Remote Users Deny Service | SECTRACK | securitytracker.com |
| SCOSA-2006.6 | SCO | ftp.sco.com |
| Debian -- Security Information -- DSA-763-1 zlib | DEBIAN | www.debian.org |
| Webmail - OVH | VUPEN | www.vupen.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[672376](#) EulerOS Security Update for deltarpm (EulerOS-SA-2022-2723)

[672379](#) EulerOS Security Update for deltarpm (EulerOS-SA-2022-2758)

[672438](#) EulerOS Security Update for deltarpm (EulerOS-SA-2022-2841)

[672469](#) EulerOS Security Update for deltarpm (EulerOS-SA-2022-2816)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)