



CVE-2006-4336

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

Summary

CVE	CVE-2006-4336
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-19 21:07:00 UTC
Updated	2018-10-17 21:34:00 UTC
Description	Buffer underflow in the build_tree function in unpack.c in gzip 1.3.5 allows context-dependent attackers to execute arbitrary

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gzip	Gzip	1.3.5	All	All	All
Application	Gzip	Gzip	1.3.5	All	All	All

References

Reference
OpenPKG Corporation: Security: Security Advisories
Webmail - OVH
VMware ESX Server 2.5.4 Upgrade Patch 5 (for 2.5.4 Systems Only)
2006-0052
Red Hat update for gzip - Advisories - Secunia
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia
Advisories - Mandriva Linux
rPath update for gzip - Advisories - Secunia
SecurityFocus
IBM X-Force Exchange
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia
The Slackware Linux Project: Slackware Security Advisories

US-CERT Technical Cyber Security Alert TA06-333A -- Apple Releases Security Update to Address Multiple Vulnerabilities
US-CERT Vulnerability Note VU#554780
GNU GZip Archive Handling Multiple Remote Vulnerabilities
Slackware update for gzip - Advisories - Secunia
Gentoo update for gzip - Advisories - Secunia
Webmail - OVH
SecurityFocus
Avaya Products gzip Multiple Vulnerabilities - Advisories - Secunia
HP Tru64 UNIX gzip Multiple Vulnerabilities - Advisories - Secunia
Webmail - OVH
Webmail - OVH
usn/usn-349-1 - Ubuntu: Linux for human beings
APPLE-SA-2006-11-28 Security Update 2006-007
HP-UX update for GZIP - Advisories - Secunia
Webmail - OVH
Gentoo Linux Documentation -- LHa: Multiple vulnerabilities
gzip Multiple Vulnerabilities - Advisories - Secunia
[#RPL-615] multiple vulnerabilities in gzip: CVE-2006-4334 CVE-2006-4335 CVE-2006-4336 CVE-2006-4337 CVE-2006-4338 - rPath JIRA
rhnl.redhat.com Red Hat Support
Mandriva update for gzip - Advisories - Secunia
20061001-01-P
204676 – CVE-2006-4334 gzip multiple issues (CVE-2006-4335, CVE-2006-4336, CVE-2006-4337, CVE-2006-4338)
LHa Multiple Vulnerabilities - Advisories - Secunia
ASA-2006-218 (RHSA-2006-0667)
Gentoo update for lha - Advisories - Secunia
SUSE update for gzip - Advisories - Secunia
Repository / Oval Repository
#102766: Multiple Security Vulnerabilities in the gzip(1) Command May Lead to Denial of Service (DoS) or Execution of Arbitrary Code
SecurityFocus
SecurityFocus
About the security content of Security Update 2006-007
FreeBSD update for gzip - Advisories - Secunia
VMware ESX Server Multiple Security Updates - Advisories - Secunia
SecurityTracker.com Archives - Gzip Bugs in Expanding Archives Let Remote Users Cause Denial of Service Conditions or Arbitrary Code Ex
Debian update for gzip - Advisories - Secunia
SecurityTracker.com Archives - Gzip Bugs in Expanding Archives Let Remote Users Cause Denial of Service Conditions or Arbitrary Code Ex

Sun Solaris update for gzip - Advisories - Secunia
Security Announcement
SecurityFocus
Gentoo Linux Documentation -- gzip: Multiple vulnerabilities
FreeBSD-SA-06:21
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Debian -- Security Information -- DSA-1181-1 gzip
Ubuntu update for gzip - Advisories - Secunia
Trustix updates for freetype / gzip - Advisories - Secunia
CVE Program record
NVD vulnerability detail
◀

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

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](#)