



CVE-2005-0953

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2005-0953
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2018-10-19 15:31:00 UTC
Description	Race condition in bzip2 1.0.2 and earlier allows local users to modify permissions of arbitrary files via a hard link attack on e

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bzip	Bzip2	0.9	All	All	All
Application	Bzip	Bzip2	0.9.5_a	All	All	All
Application	Bzip	Bzip2	0.9.5_b	All	All	All
Application	Bzip	Bzip2	0.9.5_c	All	All	All
Application	Bzip	Bzip2	0.9.5_d	All	All	All
Application	Bzip	Bzip2	0.9_a	All	All	All
Application	Bzip	Bzip2	0.9_b	All	All	All
Application	Bzip	Bzip2	0.9_c	All	All	All
Application	Bzip	Bzip2	1.0	All	All	All
Application	Bzip	Bzip2	1.0.1	All	All	All
Application	Bzip	Bzip2	1.0.2	All	All	All
Application	Bzip	Bzip2	0.9	All	All	All
Application	Bzip	Bzip2	0.9.5_a	All	All	All
Application	Bzip	Bzip2	0.9.5_b	All	All	All
Application	Bzip	Bzip2	0.9.5_c	All	All	All
Application	Bzip	Bzip2	0.9.5_d	All	All	All
Application	Bzip	Bzip2	0.9_a	All	All	All

Application	Bzip	Bzip2	0.9_b	All	All	All
Application	Bzip	Bzip2	0.9_c	All	All	All
Application	Bzip	Bzip2	1.0	All	All	All
Application	Bzip	Bzip2	1.0.1	All	All	All
Application	Bzip	Bzip2	1.0.2	All	All	All

References

Reference

[APPLE-SA-2007-11-14 Mac OS X v10.4.11 and Security Update 2007-008](#)

[US-CERT Technical Cyber Security Alert TA07-319A -- Apple Updates for Multiple Vulnerabilities](#)

[Webmail - OVH](#)

[Apple Mac OS X v10.4.11 2007-008 Multiple Security Vulnerabilities](#)

[200191](#)

[IBM X-Force Exchange](#)

[Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia](#)

[NetBSD update for bzip2 - Advisories - Secunia](#)

[Advisories - Mandriva Linux](#)

[rhn.redhat.com | Red Hat Support](#)

[bzip2 chmod File Permission Modification Race Condition Weakness](#)

[Sun Solaris bzip2 Multiple Vulnerabilities - Advisories - Secunia](#)

['bzip2 TOCTOU file-permissions vulnerability' - MARC](#)

[Debian -- Security Information -- DSA-730-1 bzip2](#)

[Repository / Oval Repository](#)

[The Fedora Legacy Project](#)

[NetBSD-SA2008-004](#)

[OpenPKG Corporation: Security: Security Advisories](#)

[Repository / Oval Repository](#)

[SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia](#)

[#200191: Two Security Vulnerabilities in the bzip2\(1\) Command may Allow the Permissions of Arbitrary Files to be Modified or Allow for Arbitr](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[SecurityFocus](#)

[20060301-01-U](#)

[About the security content of Mac OS X 10.4.11 and Security Update 2007-008](#)

[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](#).

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