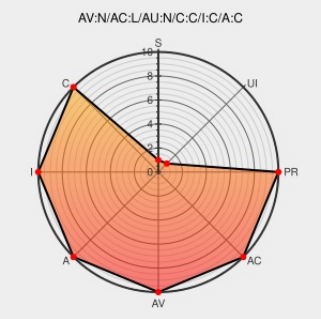
CVE-2004-0769

Published on: 08/04/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:11 PM UTC

CVE-2004-0769

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Bugzilla from Mozilla contain the following vulnerability:

Buffer overflow in LHA allows remote attackers to execute arbitrary code via long pathnames in LHarc format 2 headers for a .LHZ archive, as originally demonstrated using the "x" option but also exploitable through "l" and "v", and fixed in header.c, a different issue than CVE-2004-0771.

CVE-2004-0769 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Support	www.redhat.com text/html	REDHAT RHSA-2004:323
Gentoo Bug 51285 - app-arch/lha : buffer overflow again	Exploit Patch Vendor Advisory bugs.gentoo.org text/html	CONFIRM bugs.gentoo.org/show_bug.cgi?id=51285
No Description Provided	bugzilla.fedora.us Inactive Link Not Archived	FEDORA FLSA:1833
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2004:440

Gentoo Linux Documentation -- LHa: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-200409-13
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11047
	lw.ftw.zamosc.pl text/plain Inactive Link Not Archived	MISC lw.ftw.zamosc.pl/lha-exploit.txt
'Re: [SECURITY] [DSA 515-1] New lha packages fix several vulnerabilities; Re:' - MARC	marc.info text/html	BUGTRAQ 20040616 Re: [SECURITY] [DSA 515-1] New lha packages fix several vulnerabilities; Re:
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF lha-long-pathname-bo(16917)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Bugzilla	All	All	All	All
Application	Mozilla	Bugzilla	All	All	All	All

cpe:2.3:a:mozilla:bugzilla:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:bugzilla:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→