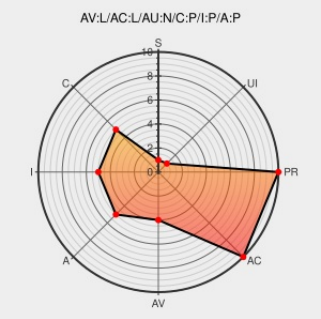
CVE-1999-1048

Published on: 09/05/1998 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:32 PM UTC

CVE-1999-1048

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

Buffer overflow in bash 2.0.0, 1.4.17, and other versions allows local attackers to gain privileges by creating an extremely large directory name, which is inserted into the password prompt via the \w option in the PS1 environmental variable when another user changes into that directory.

CVE-1999-1048 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian GNU/Linux -- Security Information -- bash	Patch, Vendor Advisory, www.debian.org, Depreciated Link, text/html	DEBIAN 19980909 problem with very long pathnames
SecurityFocus	Exploit, Vendor Advisory, www.securityfocus.com, text/html	BUGTRAQ 19980905 BASH buffer overflow, LiNUX x86 exploit
	marc.info, text/x-c	BUGTRAQ 19970821 Buffer overflow in /bin/bash
IBM X-Force Exchange	exchange.xforce.ibmcloud.com	XF linux-bash-bo(3414)

	text/html	
No Description Provided	www.osvdb.org	OSVDB 8345
	Inactive Link Not Archived	

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	1.3.1	All	All	All
Operating System	Debian	Debian Linux	1.3.1	All	All	All
Operating System	Redhat	Linux	4.2	All	All	All
Operating System	Redhat	Linux	4.2	All	All	All

cpe:2.3:o:debian:debian_linux:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:4.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:4.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→