



CVE-2002-1368

Published on: 12/20/2002 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

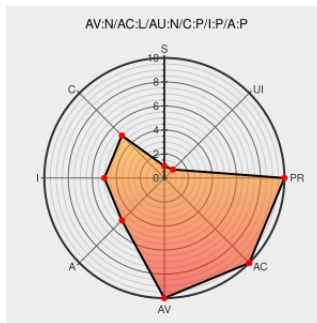
CVE-2002-1368

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Mac Os X](#) from [Apple](#) contain the following vulnerability:

Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by causing negative arguments to be fed into memcpy() calls via HTTP requests with (1) a negative Content-Length value or (2) a negative length in a chunked transfer encoding.

CVE-2002-1368 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Advisories - Mandriva

[www.mandriva.com](#)
[text/html](#)

[MANDRAKE MDKSA-2003:001](#)

Secunia - Advisories - CUPS
multiple vulnerabilities

[web.archive.org](#)
[text/html](#)

[SECUNIA 7756](#)

No Description Provided

[marc.info](#)
[text/html](#)

[BUGTRAQ 20021219 iDEFENSE Security Advisory 12.19.02: Multiple Security Vulnerabilities in Common Unix Printing System \(CUPS\)](#)

No Description Provided

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[VULNWATCH 20021219 iDEFENSE Security Advisory 12.19.02: Multiple Security Vulnerabilities in Common Unix Printing System \(CUPS\)](#)

Accenture | Let there be
change

[Exploit](#)
[Vendor Advisory](#)

[MISC www.idefense.com/advisory/12.19.02.txt](#)

	www.idefense.com text/plain	
Secunia - Advisories - RedHat updates to CUPS	web.archive.org text/html	 SECUNIA 7858
Secunia - Advisories - Gentoo updates to CUPS	web.archive.org text/html	 SECUNIA 7794
Secunia - Advisories - Debian updates to cupsys	web.archive.org text/html	 SECUNIA 7907
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2002:295
Secunia - Advisories - OpenLinux updates to CUPS	web.archive.org text/html	 SECUNIA 7913
NOVELL: Broken Link - 404 Error Pages	web.archive.org text/html Inactive Link Not Archived	 SUSE SuSE-SA:2003:002
	ftp.sco.com text/plain	 CALDERA CSSA-2003-004.0
Secunia - Advisories - Mandrake updates to CUPS	web.archive.org text/html	 SECUNIA 7843
Secunia - Advisories - Debian updates for CUPS	web.archive.org text/html	 SECUNIA 8080
Debian -- Security Information -- DSA-232-1 cupsys	www.debian.org Depreciated Link text/html	 DEBIAN DSA-232
Home - Conectiva	distro.conectiva.com.br text/html	 CONECTIVA CLSA-2003:702
Secunia - Advisories - Conectiva update for CUPS	web.archive.org text/html	 SECUNIA 9325
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF cups-neg-memcpy-bo(10909)
Secunia - Advisories - SuSE updates to CUPS	web.archive.org text/html	 SECUNIA 7803
CUPS Negative Length HTTP Header Vulnerability	cve.report (archive) text/html	 BID 6437

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	Apple	Mac Os X	10.2	All	All	All
Operating	Apple	Mac Os X	10.2.2	All	All	All

cpe:2.3:a:easy_software_products:cups:1.0.4:*****:

cpe:2.3:a:easy_software_products:cups:1.0.4_8:*****:

cpe:2.3:a:easy_software_products:cups:1.1.1:*****:

cpe:2.3:a:easy_software_products:cups:1.1.10:*****:

cpe:2.3:a:easy_software_products:cups:1.1.13:*****:

cpe:2.3:a:easy_software_products:cups:1.1.14:*****:

cpe:2.3:a:easy_software_products:cups:1.1.17:*****:

cpe:2.3:a:easy_software_products:cups:1.1.4:*****:

cpe:2.3:a:easy_software_products:cups:1.1.4_2:*****:

cpe:2.3:a:easy_software_products:cups:1.1.4_3:*****:

cpe:2.3:a:easy_software_products:cups:1.1.4_5:*****:

cpe:2.3:a:easy_software_products:cups:1.1.6:*****:

cpe:2.3:a:easy_software_products:cups:1.1.7:*****:

cpe:2.3:a:easy_software_products:cups:1.0.4:*****:

cpe:2.3:a:easy_software_products:cups:1.0.4_8:*****:

cpe:2.3:a:easy_software_products:cups:1.1.1:*****:

cpe:2.3:a:easy_software_products:cups:1.1.10:*****:

cpe:2.3:a:easy_software_products:cups:1.1.13:*****:

cpe:2.3:a:easy_software_products:cups:1.1.14:*****:

cpe:2.3:a:easy_software_products:cups:1.1.17:*****:

cpe:2.3:a:easy_software_products:cups:1.1.4:*****:

cpe:2.3:a:easy_software_products:cups:1.1.4_2:*****:

cpe:2.3:a:easy_software_products:cups:1.1.4_3:*****:

cpe:2.3:a:easy_software_products:cups:1.1.4_5:*****:

cpe:2.3:a:easy_software_products:cups:1.1.6:*****:

cpe:2.3:a:easy_software_products:cups:1.1.7:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)