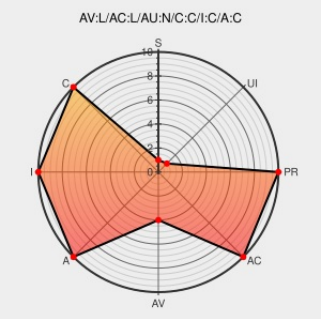
CVE-2002-1384

Published on: 01/02/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1384

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



Certain versions of Cups from Easy Software Products contain the following vulnerability:

Integer overflow in pdftops, as used in Xpdf 2.01 and earlier, xpdf-i, and CUPS before 1.1.18, allows local users to execute arbitrary code via a ColorSpace entry with a large number of elements, as demonstrated by cups-pdf.

CVE-2002-1384 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-222-1 xpdf	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-222
redhat.com | Red Hat Support	www.redhat.com, text/html	REDHAT RHSA-2002:295
redhat.com | Red Hat Support	www.redhat.com, text/html	REDHAT RHSA-2002:307
'GLSA: xpdf' - MARC	marc.info, text/html	GENTOO GLSA-200301-1
Accenture | Let there be change	Exploit, Patch, Vendor Advisory, www.idefense.com	MISC www.idefense.com/advisory/12.23.02.txt

	text/plain	
Mandrakesoft Security Advisories	web.archive.org text/html Inactive Link Not Archived	MANDRAKE MDKSA-2003:002
Xpdf/CUPS pdftops Integer Overflow Vulnerability	cve.report (archive) text/html	BID 6475
Mandrakesoft Security Advisories	web.archive.org text/html Inactive Link Not Archived	MANDRAKE MDKSA-2003:001
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF pdftops-integer-overflow(10937)
Debian -- Security Information -- DSA-232-1 cupsys	www.debian.org Depreciated Link text/html	DEBIAN DSA-232
NOVELL: Broken Link - 404 Error Pages	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2003:002
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:037
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:216
Debian -- Security Information -- DSA-226-1 xpdf-i	www.debian.org Depreciated Link text/html	DEBIAN DSA-226

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Easy Software Products	Cups	1.0.4	All	All	All
Application	Easy Software Products	Cups	1.0.4_8	All	All	All
Application	Easy Software Products	Cups	1.1.1	All	All	All
Application	Easy Software Products	Cups	1.1.10	All	All	All
Application	Easy Software Products	Cups	1.1.13	All	All	All
Application	Easy Software Products	Cups	1.1.14	All	All	All
Application	Easy Software Products	Cups	1.1.17	All	All	All
Application	Easy Software Products	Cups	1.1.4	All	All	All
Application	Easy Software Products	Cups	1.1.4_2	All	All	All
Application	Easy Software Products	Cups	1.1.4_3	All	All	All

Application	Easy Software Products	Cups	1.1.4_5	All	All	All
Application	Easy Software Products	Cups	1.1.6	All	All	All
Application	Easy Software Products	Cups	1.1.7	All	All	All
Application	Easy Software Products	Cups	1.0.4	All	All	All
Application	Easy Software Products	Cups	1.0.4_8	All	All	All
Application	Easy Software Products	Cups	1.1.1	All	All	All
Application	Easy Software Products	Cups	1.1.10	All	All	All
Application	Easy Software Products	Cups	1.1.13	All	All	All
Application	Easy Software Products	Cups	1.1.14	All	All	All
Application	Easy Software Products	Cups	1.1.17	All	All	All
Application	Easy Software Products	Cups	1.1.4	All	All	All
Application	Easy Software Products	Cups	1.1.4_2	All	All	All
Application	Easy Software Products	Cups	1.1.4_3	All	All	All
Application	Easy Software Products	Cups	1.1.4_5	All	All	All
Application	Easy Software Products	Cups	1.1.6	All	All	All
Application	Easy Software Products	Cups	1.1.7	All	All	All
Application	Xpdf	Xpdf	0.90	All	All	All
Application	Xpdf	Xpdf	0.91	All	All	All
Application	Xpdf	Xpdf	1.0	All	All	All
Application	Xpdf	Xpdf	1.0a	All	All	All
Application	Xpdf	Xpdf	1.1	All	All	All
Application	Xpdf	Xpdf	2.0	All	All	All
Application	Xpdf	Xpdf	2.1	All	All	All
Application	Xpdf	Xpdf	0.90	All	All	All
Application	Xpdf	Xpdf	0.91	All	All	All
Application	Xpdf	Xpdf	1.0	All	All	All
Application	Xpdf	Xpdf	1.0a	All	All	All
Application	Xpdf	Xpdf	1.1	All	All	All
Application	Xpdf	Xpdf	2.0	All	All	All
Application	Xpdf	Xpdf	2.1	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:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:0.90:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:0.91:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:1.0a:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:0.90:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:0.91:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:1.0a:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:xpdf:xpdf:2.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→