



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 [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Debian -- Security Information -- DSA-222-1 xpdf

[www.debian.org](#)
Deprecated 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](#) [MANDRAKE MDKSA-2003:002](#)[text/html](#)[Inactive Link](#) [Not Archived](#)

Xpdf/CUPS pdftops Integer Overflow Vulnerability

[cve.report \(archive\)](#) [BID 6475](#)[text/html](#)

Mandrakesoft Security Advisories

[web.archive.org](#) [MANDRAKE MDKSA-2003:001](#)[text/html](#)[Inactive Link](#) [Not Archived](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#) [XF pdftops-integer-overflow\(10937\)](#)[text/html](#)

Debian -- Security Information -- DSA-232-1 cupsys

[www.debian.org](#) [DEBIAN DSA-232](#)[Deprecated Link](#)[text/html](#)

NOVELL: Broken Link - 404 Error Pages

[web.archive.org](#) [SUSE SUSE-SA:2003:002](#)[text/html](#)[Inactive Link](#) [Not Archived](#)

redhat.com | Red Hat Support

[www.redhat.com](#) [REDHAT RHSA-2003:037](#)[text/html](#)

redhat.com | Red Hat Support

[www.redhat.com](#) [REDHAT RHSA-2003:216](#)[text/html](#)

Debian -- Security Information -- DSA-226-1 xpdf-i

[www.debian.org](#) [DEBIAN DSA-226](#)[Deprecated Link](#)[text/html](#)

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
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 →](#)