# CVE-2008-1693

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2008-1693 |
| **State** | PUBLIC |
| **Assigner** | security@ubuntu.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2008-04-18 15:05:00 UTC |
| **Updated** | 2017-09-29 01:30:00 UTC |
| **Description** | The CairoFont::create function in CairoFontEngine.cc in Poppler, possibly before 0.8.0, as used in Xpdf, Evince, ePDFview |

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Poppler | Poppler | 0.1 | All | All | All |
| Application | Poppler | Poppler | 0.1.1 | All | All | All |
| Application | Poppler | Poppler | 0.1.2 | All | All | All |
| Application | Poppler | Poppler | 0.2.0 | All | All | All |
| Application | Poppler | Poppler | 0.3.0 | All | All | All |
| Application | Poppler | Poppler | 0.3.1 | All | All | All |
| Application | Poppler | Poppler | 0.3.2 | All | All | All |
| Application | Poppler | Poppler | 0.3.3 | All | All | All |
| Application | Poppler | Poppler | 0.4.0 | All | All | All |
| Application | Poppler | Poppler | 0.4.1 | All | All | All |
| Application | Poppler | Poppler | 0.4.2 | All | All | All |
| Application | Poppler | Poppler | 0.4.3 | All | All | All |
| Application | Poppler | Poppler | 0.4.4 | All | All | All |
| Application | Poppler | Poppler | 0.5.0 | All | All | All |
| Application | Poppler | Poppler | 0.5.1 | All | All | All |
| Application | Poppler | Poppler | 0.5.2 | All | All | All |
| Application | Poppler | Poppler | 0.5.3 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Poppler | Poppler | 0.5.4 | All | All | All |
| Application | Poppler | Poppler | 0.5.9 | All | All | All |
| Application | Poppler | Poppler | 0.5.91 | All | All | All |
| Application | Poppler | Poppler | 0.6.0 | All | All | All |
| Application | Poppler | Poppler | 0.6.1 | All | All | All |
| Application | Poppler | Poppler | 0.6.2 | All | All | All |
| Application | Poppler | Poppler | 0.6.3 | All | All | All |
| Application | Poppler | Poppler | 0.6.4 | All | All | All |
| Application | Poppler | Poppler | 0.7.0 | All | All | All |
| Application | Poppler | Poppler | 0.7.1 | All | All | All |
| Application | Poppler | Poppler | 0.7.2 | All | All | All |
| Application | Poppler | Poppler | All | All | All | All |
| Application | Poppler | Poppler | 0.1 | All | All | All |
| Application | Poppler | Poppler | 0.1.1 | All | All | All |
| Application | Poppler | Poppler | 0.1.2 | All | All | All |
| Application | Poppler | Poppler | 0.2.0 | All | All | All |
| Application | Poppler | Poppler | 0.3.0 | All | All | All |
| Application | Poppler | Poppler | 0.3.1 | All | All | All |
| Application | Poppler | Poppler | 0.3.2 | All | All | All |
| Application | Poppler | Poppler | 0.3.3 | All | All | All |
| Application | Poppler | Poppler | 0.4.0 | All | All | All |
| Application | Poppler | Poppler | 0.4.1 | All | All | All |
| Application | Poppler | Poppler | 0.4.2 | All | All | All |
| Application | Poppler | Poppler | 0.4.3 | All | All | All |
| Application | Poppler | Poppler | 0.4.4 | All | All | All |
| Application | Poppler | Poppler | 0.5.0 | All | All | All |
| Application | Poppler | Poppler | 0.5.1 | All | All | All |
| Application | Poppler | Poppler | 0.5.2 | All | All | All |
| Application | Poppler | Poppler | 0.5.3 | All | All | All |
| Application | Poppler | Poppler | 0.5.4 | All | All | All |
| Application | Poppler | Poppler | 0.5.9 | All | All | All |
| Application | Poppler | Poppler | 0.5.91 | All | All | All |
| Application | Poppler | Poppler | 0.6.0 | All | All | All |
| Application | Poppler | Poppler | 0.6.1 | All | All | All |
| Application | Poppler | Poppler | 0.6.2 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Poppler | Poppler | 0.6.3 | All | All | All |
| Application | Poppler | Poppler | 0.6.4 | All | All | All |
| Application | Poppler | Poppler | 0.7.0 | All | All | All |
| Application | Poppler | Poppler | 0.7.1 | All | All | All |
| Application | Poppler | Poppler | 0.7.2 | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| [security-announce] SUSE Security Summary Report SUSE-SR:200?8:011 | SUSE | lists.op |
| Ubuntu update for KOffice - Advisories - Secunia | SECUNIA | secuni |
| Debian update for xpdf - Advisories - Secunia | SECUNIA | secuni |
| rhn.redhat.com \| Red Hat Support | REDHAT | www.r |
| Poppler Embedded Fonts Processing Vulnerability - Advisories - Secunia | SECUNIA | secuni |
| Support / Security / Advisories / / MDVSA-2008:173 \| Mandriva | MANDRIVA | www.r |
| Poppler: User-assisted execution of arbitrary code — Gentoo Linux Documentation | GENTOO | securit |
| Poppler and Xpdf PDF Rendering Library Embedded Font Remote Code Execution Vulnerability | BID | www.s |
| SecurityTracker.com Archives - Xpdf Bug in Processing Embedded Fonts Lets Remote Users Execute Arbitrary Code | SECTRACK | securit |
| Red Hat update for poppler - Advisories - Secunia | SECUNIA | secuni |
| rhn.redhat.com \| Red Hat Support | REDHAT | www.r |
| Xpdf Embedded Fonts Processing Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secuni |
| Debian -- Security Information -- DSA-1548-1 xpdf | DEBIAN | www.c |
| Red Hat update for xpdf - Advisories - Secunia | SECUNIA | secuni |
| IBM X-Force Exchange | XF | excha |
| Ubuntu update for poppler - Advisories - Secunia | SECUNIA | secuni |
| Security Announcement | SUSE | www.r |
| Support / Security / Advisories / / MDVSA-2008:197 \| Mandriva | MANDRIVA | www.r |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN | www.v |
| Repository / Oval Repository | OVAL | oval.ci |
| [SECURITY] Fedora 7 Update: poppler-0.5.4-9.fc7 | FEDORA | www.r |
| SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secuni |
| Fedora update for poppler - Advisories - Secunia | SECUNIA | secuni |
| rhn.redhat.com \| Red Hat Support | REDHAT | www.r |
| rhn.redhat.com \| Red Hat Support | REDHAT | www.r |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN | www.v |
| Red Hat update for gpdf - Advisories - Secunia | SECUNIA | secuni |
| Debian update for poppler - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secuni |

| | | |
|---|---|---|
| Advisories \| Mandriva | MANDRIVA | www.m |
| USN-603-2: KOffice vulnerability \| Ubuntu | UBUNTU | www.u |
| Debian -- Security Information -- DSA-1606-1 poppler | DEBIAN | www.d |
| USN-603-1: poppler vulnerability \| Ubuntu | UBUNTU | www.u |
| Gentoo update for poppler - Advisories - Secunia | SECUNIA | secuni |
| Red Hat update for kdegraphics - Advisories - Secunia | SECUNIA | secuni |
| CVE Program record | CVE.ORG | www.c |
| NVD vulnerability detail | NVD | nvd.nis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.