



# CVE-2006-2193

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2006-2193   |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | debian  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2006-06-08 19:06:00 UTC   |
| <b>Updated</b>         | 2025-04-03 01:03:51 UTC   |
| <b>Description</b>     | Buffer overflow in the t2p_write_pdf_string function in tiff2pdf in libtiff 3.8.2 and earlier allows attackers to cause a denial of |

## Risk And Classification

**Primary CVSS:** v2.0 7.5 from nvd@nist.gov

**AV:N/AC:L/Au:N/C:P/I:P/A:P**

**EPSS:** 0.006400000 probability, percentile 0.705680000 (date 2026-04-20)

**Problem Types:** NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

**Network**

Access Complexity

**Low**

Authentication

**None**

Confidentiality

**Partial**

Integrity

**Partial**

Availability

**Partial**

**AV:N/AC:L/Au:N/C:P/I:P/A:P**

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------|--------|---------|---------|--------|---------|----------|
|------|--------|---------|---------|--------|---------|----------|

|             |         |         |       |     |     |     |
|-------------|---------|---------|-------|-----|-----|-----|
| Application | Libtiff | Libtiff | 3.4   | All | All | All |
| Application | Libtiff | Libtiff | 3.5.1 | All | All | All |
| Application | Libtiff | Libtiff | 3.5.2 | All | All | All |
| Application | Libtiff | Libtiff | 3.5.3 | All | All | All |
| Application | Libtiff | Libtiff | 3.5.4 | All | All | All |
| Application | Libtiff | Libtiff | 3.5.5 | All | All | All |
| Application | Libtiff | Libtiff | 3.5.6 | All | All | All |
| Application | Libtiff | Libtiff | 3.5.7 | All | All | All |
| Application | Libtiff | Libtiff | 3.6.0 | All | All | All |
| Application | Libtiff | Libtiff | 3.6.1 | All | All | All |
| Application | Libtiff | Libtiff | 3.7.0 | All | All | All |
| Application | Libtiff | Libtiff | 3.7.1 | All | All | All |
| Application | Libtiff | Libtiff | 3.8.0 | All | All | All |
| Application | Libtiff | Libtiff | 3.8.1 | All | All | All |
| Application | Libtiff | Libtiff | All   | All | All | All |

### Vendor Declared Affected Products

| Source | Vendor | Product | Version      | Platforms     |
|--------|--------|---------|--------------|---------------|
| CNA    | Na     | N/a     | affected n/a | Not specified |

### References

| Reference   | Source                  |
|---|-------------------------|
| Webmail - OVH   | af854a3a-2127-422b-91ae |
| Webmail - OVH   | af854a3a-2127-422b-91ae |
| Sun Solaris libTIFF Multiple Vulnerabilities - Advisories - Secunia   | af854a3a-2127-422b-91ae |
| Advisories - Mandriva Linux   | af854a3a-2127-422b-91ae |
| IBM X-Force Exchange  | af854a3a-2127-422b-91ae |
| Gentoo Linux Documentation -- libTIFF: Multiple buffer overflows      | af854a3a-2127-422b-91ae |
| bugzilla.remotesensing.org/show_bug.cgi                               | af854a3a-2127-422b-91ae |
| LibTIFF tiff2pdf Buffer Overflow Vulnerability - Advisories - Secunia | af854a3a-2127-422b-91ae |
| Ubuntu update for tiff - Advisories - Secunia                         | af854a3a-2127-422b-91ae |
| USN-289-1: tiff vulnerabilities   Ubuntu security notices             | af854a3a-2127-422b-91ae |
| Secunia - Advisories - Mandriva update for libtiff                    | af854a3a-2127-422b-91ae |
| sunsolve.sun.com/search/document.do                                   | af854a3a-2127-422b-91ae |
| Webmail - OVH   | af854a3a-2127-422b-91ae |
| #370355 - libtiff-tools: tiff2pdf segfault - Debian Bug report logs   | af854a3a-2127-422b-91ae |

|   |                         |
|---|-------------------------|
| Gentoo update for tiff - Advisories - Secunia   | af854a3a-2127-422b-91ae |
| Sun Solaris libtiff Multiple Vulnerabilities - Advisories - Secunia                                 | af854a3a-2127-422b-91ae |
| Debian -- Security Information -- DSA-1091-1 tiff   | af854a3a-2127-422b-91ae |
| Support   | af854a3a-2127-422b-91ae |
| SuSE Security announcements: [suse-security-announce] SUSE Security Summary Report SUSE-SR:2006:014 | af854a3a-2127-422b-91ae |
| LibTIFF tiff2pdf Remote Buffer Overflow Vulnerability   | af854a3a-2127-422b-91ae |
| Debian update for tiff - Advisories - Secunia   | af854a3a-2127-422b-91ae |
| Sun Solaris libtiff Multiple Vulnerabilities - Advisories - Secunia                                 | af854a3a-2127-422b-91ae |
| sunsolve.sun.com/search/document.do   | af854a3a-2127-422b-91ae |
| Repository / Oval Repository  | af854a3a-2127-422b-91ae |
| SUSE Updates for Multiple Packages - Advisories - Secunia   | af854a3a-2127-422b-91ae |
| Red Hat update for libtiff - Secunia Advisories - Vulnerability Intelligence - Secunia.com          | af854a3a-2127-422b-91ae |
| CVE Program record  | CVE.ORG                 |
| NVD vulnerability detail  | NVD                     |

### Vendor Comments And Credit

| Organization | Published  | Contributor | Statement   |
|--------------|------------|-------------|---|
| Red Hat      | 2008-09-02 | Mark J Cox  | This issue does not affect Red Hat Enterprise Linux 2.1 and 3 This issue was addressed in Red |

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

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)