



# Gimp: gimp:memory disclosure and denial of service via specially crafted pcx image

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-4887  |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | redhat   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2026-03-26 13:16:30 UTC  |
| <b>Updated</b>         | 2026-04-20 13:11:24 UTC  |
| <b>Description</b>     | A flaw was found in GIMP. This issue is a heap buffer over-read in GIMP PCX file loader due to an off-by-one error. A remote |

## Risk And Classification

**Primary CVSS:** v3.1 7.1 HIGH from nvd@nist.gov

**CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H**

**Problem Types:** CWE-193 | CWE-193 Off-by-one Error

| Version | Source              | Type      | Score | Severity | Vector  |
|---------|---------------------|-----------|-------|----------|---|
| 3.1     | nvd@nist.gov        | Primary   | 7.1   | HIGH     | <b>CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H</b> |
| 3.1     | secalert@redhat.com | Secondary | 6.1   | MEDIUM   | <b>CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H</b> |
| 3.1     | CNA                 | CVSS      | 6.1   | MEDIUM   | <b>CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H</b> |

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H

### NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product          | Version | Update | Edition | Language |
|------------------|--------|------------------|---------|--------|---------|----------|
| Application      | Gimp   | Gimp             | All     | All    | All     | All      |
| Application      | Gimp   | Gimp             | 3.2.0   | rc1    | All     | All      |
| Application      | Gimp   | Gimp             | 3.2.0   | rc2    | All     | All      |
| Application      | Gimp   | Gimp             | 3.2.0   | rc3    | All     | All      |
| Operating System | Redhat | Enterprise Linux | 6.0     | All    | All     | All      |
| Operating System | Redhat | Enterprise Linux | 7.0     | All    | All     | All      |
| Operating System | Redhat | Enterprise Linux | 8.0     | All    | All     | All      |
| Operating System | Redhat | Enterprise Linux | 9.0     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor  | Product                    | Version       | Platforms     |
|--------|---------|----------------------------|---------------|---------------|
| CNA    | Red Hat | Red Hat Enterprise Linux 6 | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 7 | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 8 | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 9 | Not specified | Not specified |

### References

| Reference   | Source              | Link  | Tags                            |
|---|---------------------|---|---------------------------------|
| <a href="https://access.redhat.com/security/cve/CVE-2026-4887">access.redhat.com/security/cve/CVE-2026-4887</a> | secalert@redhat.com | <a href="https://access.redhat.com">access.redhat.com</a>     | Mitigation, Vendor Advisory     |
| <a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>                         | secalert@redhat.com | <a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a> | Issue Tracking, Vendor Advisory |
| <a href="https://gitlab.gnome.org/GNOME/gimp/-/issues/15960">gitlab.gnome.org/GNOME/gimp/-/issues/15960</a>     | secalert@redhat.com | <a href="https://gitlab.gnome.org">gitlab.gnome.org</a>       | Exploit, Issue Tracking         |
| CVE Program record  | CVE.ORG             | <a href="https://www.cve.org">www.cve.org</a>                 | canonical                       |
| NVD vulnerability detail  | NVD                 | <a href="https://nvd.nist.gov">nvd.nist.gov</a>               | canonical, analysis             |

### Vendor Comments And Credit

Discovery Credit

**CNA:** Red Hat would like to thank Meshaal (@unrealmesh) for reporting this issue. (en)

### Additional Advisory Data

| Source | Time                     | Event                |
|--------|--------------------------|----------------------|
| CNA    | 2026-03-26T11:34:22.208Z | Reported to Red Hat. |
| CNA    | 2026-03-26T11:35:00.070Z | Made public.         |

#### Workarounds

**CNA:** Users should avoid opening untrusted PCX image files with GIMP. If GIMP is not required, consider removing the `gimp` package to eliminate this attack vector.

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](#)