



# Gimp: gimp: denial of service due to stack buffer overflow in tim image loader

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

## Summary

<b>CVE</b>	CVE-2026-40916
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-15 20:16:36 UTC
<b>Updated</b>	2026-04-17 15:08:01 UTC

**Description** A flaw was found in GIMP. A stack buffer overflow vulnerability in the TIM image loader's 4BPP decoding path allows a local

## Risk And Classification

**Primary CVSS:** v3.1 5 MEDIUM from secalert@redhat.com

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

**EPSS:** 0.000050000 probability, percentile 0.002500000 (date 2026-04-20)

**Problem Types:** CWE-787 | CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### 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
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-40916	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Red Hat would like to thank Mehtab Zafar for reporting this issue. (en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-04-15T18:34:57.691Z	Reported to Red Hat.
CNA	2026-04-15T18:41:43.948Z	Made public.

#### Workarounds

**CNA:** To mitigate this issue, users should avoid opening untrusted TIM image files with GIMP. As a general security practice, users should exercise caution when handling files from unknown or suspicious sources.

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

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](#)