Gimp: gimp: application crashes or information disclosure via crafted icns image files

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

Summary

CVE	CVE-2026-40917
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 20:16:37 UTC
Updated	2026-04-17 15:08:01 UTC
Description	A flaw was found in GIMP. This vulnerability, a heap buffer over-read in the `icns_slurp()` function, occurs when processing

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: 0.000130000 probability, percentile 0.020240000 (date 2026-04-20)

Problem Types: CWE-125 | CWE-125 Out-of-bounds Read

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

ntegrity

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
access.redhat.com/security/cve/CVE-2026-40917	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.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	2026-04-15T18:35:00.781Z	Reported to Red Hat.
CNA	2026-04-15T18:41:42.324Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base, or stability.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**