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

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

Summary

CVE	CVE-2026-4887
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 13:16:30 UTC
Updated	2026-04-20 13:11:24 UTC
Description	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 remo

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	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H
3.1	secalert@redhat.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

None

vailability

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
access.redhat.com/security/cve/CVE-2026-4887	secalert@redhat.com	access.redhat.com	Mitigation, Vendor Advisory
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Vendor Advisory
gitlab.gnome.org/GNOME/gimp/-/issues/15960	secalert@redhat.com	gitlab.gnome.org	Exploit, Issue Tracking
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 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.