CVE

VEX
Public o
Last mo

Jump to section

Description

A flaw was found in GIMP. An integer overflow vulnerability exists in the GIMP "Despeckle" plug-in. The issue occurs due to unchecked multiplication of image dimensions, such as width, height, and bytes-per-pixel (img_bpp), which can result in allocating insufficient memory and subsequently performing out-of-bounds writes. This issue could lead to heap corruption, a potential denial of service (DoS), or arbitrary code execution in certain scenarios.

Mitigation

Currently, no mitigation is available for this vulnerability.

Additional information

- Bugzilla 2372515: gimp: Gimp Integer Overflow
- CWE-190: Integer Overflow or Wraparound

External references

- https://www.cve.org/CVERecord?id=CVE-2025-6035
- https://nvd.nist.gov/vuln/detail/CVE-2025-6035

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State | Errata | Clear all

Products / Services	Red Hat Enterprise Linux 6
Components	gimp
State	Out of support scope
Justification	None
Errata	

Release Date	
Products / Services	Red Hat Enterprise Linux 7
Components	gimp
State	Out of support scope
Justification	None
Errata	
Release Date	
Products / Services	Red Hat Enterprise Linux 8

1-10 of 4

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

The following CVSS metrics and score provided are preliminary and subject to review.

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	6.1	7.8
Attack Vector	Local	Local
Attack Complexity	Low	Low
Privileges Required	Low	Low
User Interaction	Required	None
Scope	Unchanged	Unchanged
Confidentiality Impact	Low	High
Integrity Impact	Low	High
Availability Impact	High	High

CVSS v3 Vector

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

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

Frequently Asked Questions

- Why is Red Hat's CVSS v3 score or Impact different from other vendors?
- My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?
- What can I do if my product is listed as "Will not fix"?
- What can I do if my product is listed as "Fix deferred"?
- What is a mitigation?
- I have a Red Hat product but it is not in the above list, is it affected?
- Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?
- My product is listed as "Out of Support Scope". What does this mean?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: January 8, 2026 at 2:59:37 AM UTC

Quick Links

Help

Site Info

Related Sites

All systems operational

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie Preferences and Opt-Out Rights