



# CVE-2010-4540

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2010-4540                                                                                                              |
| <b>State</b>           | PUBLISHED                                                                                                                  |
| <b>Assigner</b>        | redhat                                                                                                                     |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2011-01-07 20:00:04 UTC                                                                                                    |
| <b>Updated</b>         | 2026-04-29 01:13:23 UTC                                                                                                    |
| <b>Description</b>     | Stack-based buffer overflow in the load_preset_response function in plug-ins/lighting/lighting-ui.c in the "LIGHTING EFPEC |

## Risk And Classification

**Primary CVSS:** v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

**Problem Types:** CWE-787 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Gimp   | Gimp    | 2.6.11  | All    | All     | All      |

| Vendor Declared Affected Products                                                            |        |         |                                     |               |
|----------------------------------------------------------------------------------------------|--------|---------|-------------------------------------|---------------|
| Source                                                                                       | Vendor | Product | Version                             | Platforms     |
| CNA                                                                                          | Na     | N/a     | affected n/a                        | Not specified |
|                                                                                              |        |         |                                     |               |
| References                                                                                   |        |         |                                     |               |
| Reference                                                                                    |        |         | Source                              |               |
| Red Hat update for gimp - Advisories - Community                                             |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| Debian -- Security Information -- DSA-2426-1 gimp                                            |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| IBM X-Force Exchange                                                                         |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| Gentoo Linux Documentation -- GIMP: Multiple vulnerabilities                                 |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| #608497 - gimp: four buffer overflows - Debian Bug report logs                               |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| Gimp Multiple Vulnerabilities - Advisories - Community                                       |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| oss-security - CVE request for buffer overflows in gimp                                      |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| Security Advisory SA48236 - Debian update for gimp - Secunia                                 |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| Support                                                                                      |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| osvdb.org/70282                                                                              |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| Security Alerts - Secunia                                                                    |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| oss-security - Re: CVE request for buffer overflows in gimp                                  |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| 666793 – (CVE-2010-4540) CVE-2010-4540 Gimp: Stack-based buffer overflow in Lighting plug-in |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2011:005                           |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                             |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| Support                                                                                      |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| Support / Security / Advisories // MDVSA-2011:103   Mandriva                                 |        |         | af854a3a-2127-422b-91ae-364da266110 |               |
| Red Hat Customer Portal                                                                      |        |         | MITRE                               |               |
| Red Hat Customer Portal                                                                      |        |         | MITRE                               |               |
| CVE-2010-4540 - Red Hat Customer Portal                                                      |        |         | MITRE                               |               |
| CVE Program record                                                                           |        |         | CVE.ORG                             |               |
| NVD vulnerability detail                                                                     |        |         | NVD                                 |               |
| <div><div></div><div></div></div>                                                            |        |         |                                     |               |
| No vendor comments have been submitted for this CVE.                                         |        |         |                                     |               |
|                                                                                              |        |         |                                     |               |
| There are currently no legacy QID mappings associated with this CVE.                         |        |         |                                     |               |

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)