



# CVE-2015-8869

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-8869
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-06-13 19:59:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	OCaml before 4.03.0 does not properly handle sign extensions, which allows remote attackers to conduct buffer overflow at

## Risk And Classification

**Problem Types:** CWE-119 | CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Application	<a href="#">Ocaml</a>	<a href="#">Ocaml</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All

## References

Reference	Source	Link	Ta
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>	
OCaml: Buffer overflow and information disclosure (GLSA 201702-15) — Gentoo Security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
Oracle Linux Bulletin - July 2016	CONFIRM	<a href="http://www.oracle.com">www.oracle.com</a>	
Red Hat Customer Portal	REDHAT	<a href="http://access.redhat.com">access.redhat.com</a>	
openSUSE-SU-2016:1335-1: moderate: Security update for ocaml	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
oss-security - buffer overflow and information leak in OCaml < 4.03.0	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
oss-security - Re: buffer overflow and information leak in OCaml < 4.03.0	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
[SECURITY] Fedora 24 Update: ocaml-4.02.3-3.fc24	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
fix PR#7003 and a few other bugs caused by misuse of Int_val · ocaml/ocaml@659615c · GitHub	CONFIRM	<a href="http://github.com">github.com</a>	

openSUSE-SU-2016:2273-1: moderate: Security update for ocaml	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>	
OCaml CVE-2015-8869 Multiple Security Vulnerabilities	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[710485](#) Gentoo Linux OCaml Buffer overflow and information disclosure Vulnerability (GLSA 201702-15)

© [CVE.report](#) 2026 |

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

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