



# CVE-2013-6393

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2013-6393
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-02-06 22:55:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	The yaml_parser_scan_tag_uri function in scanner.c in LibYAML before 0.1.5 performs an incorrect cast, which allows remote attackers to trigger a denial of service via a crafted YAML document.

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All

Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Application	<a href="#">Pyyaml</a>	<a href="#">Libyaml</a>	0.0.1	All	All	All
Application	<a href="#">Pyyaml</a>	<a href="#">Libyaml</a>	0.1.1	All	All	All
Application	<a href="#">Pyyaml</a>	<a href="#">Libyaml</a>	0.1.2	All	All	All
Application	<a href="#">Pyyaml</a>	<a href="#">Libyaml</a>	0.1.3	All	All	All
Application	<a href="#">Pyyaml</a>	<a href="#">Libyaml</a>	All	All	All	All
Application	<a href="#">Pyyaml</a>	<a href="#">Libyaml</a>	0.0.1	All	All	All
Application	<a href="#">Pyyaml</a>	<a href="#">Libyaml</a>	0.1.1	All	All	All
Application	<a href="#">Pyyaml</a>	<a href="#">Libyaml</a>	0.1.2	All	All	All
Application	<a href="#">Pyyaml</a>	<a href="#">Libyaml</a>	0.1.3	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	3.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	3.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	4.0	All	All	All

## References

Reference	Source	Link	Tag
Attachment 847926 Details for Bug 1033990 – String overflow patch	MISC	<a href="#">bugzilla.redhat.com</a>	Issue
openSUSE-SU-2015:0319-1: moderate: Security update for perl-YAML-LibYAML	SUSE	<a href="#">lists.opensuse.org</a>	This
102716	OSVDB	<a href="#">osvdb.org</a>	
openSUSE-SU-2016:1067-1: moderate: Security update for perl-YAML-LibYAML	SUSE	<a href="#">lists.opensuse.org</a>	This
xi / libyaml / Commits — Bitbucket	CONFIRM	<a href="#">bitbucket.org</a>	Issue
NEOHAPSIS - Peace of Mind Through Integrity and Insight	APPLE	<a href="#">archives.neohapsis.com</a>	Bro
NEOHAPSIS - Peace of Mind Through Integrity and Insight	APPLE	<a href="#">archives.neohapsis.com</a>	Bro
openSUSE-SU-2014:0273-1: moderate: update for libyaml	SUSE	<a href="#">lists.opensuse.org</a>	This
Debian -- Security Information -- DSA-2870-1 libyaml-libyaml-perl	DEBIAN	<a href="#">www.debian.org</a>	This
Red Hat Customer Portal	REDHAT	<a href="#">rhn.redhat.com</a>	This
Bug 1033990 – CVE-2013-6393 libyaml: heap-based buffer overflow when parsing YAML tags	CONFIRM	<a href="#">bugzilla.redhat.com</a>	Issue
USN-2098-1: LibYAML vulnerability   Ubuntu	UBUNTU	<a href="#">www.ubuntu.com</a>	This
LibYAML 'scanner.c' Remote Heap Based Buffer Overflow Vulnerability	BID	<a href="#">www.securityfocus.com</a>	This
openSUSE-SU-2014:0272-1: moderate: update for libyaml	SUSE	<a href="#">lists.opensuse.org</a>	This
Support / Security / Advisories // MDVSA-2015:060   Mandriva	MANDRIVA	<a href="#">www.mandriva.com</a>	This
CVE-2013-6393   Puppet	CONFIRM	<a href="#">puppet.com</a>	
Red Hat Customer Portal	REDHAT	<a href="#">rhn.redhat.com</a>	This
Red Hat Customer Portal	REDHAT	<a href="#">rhn.redhat.com</a>	This
Mandriva Linux - MDVSA-2015:060: High severity: libyaml: CVE-2013-6393	CONFIRM	<a href="#">www.mandriva.com</a>	This

Mageia Advisory: MGASA-2014-0040 - Updated yami packages fix CVE-2013-6393	CONFIRM	<a href="http://advisories.mageia.org">advisories.mageia.org</a>	Thi
About the security content of OS X Server v4.0 - Apple Support	CONFIRM	<a href="http://support.apple.com">support.apple.com</a>	Thi
Debian -- Security Information -- DSA-2850-1 libyaml	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Thi
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	can

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

980716 Nodejs (npm) Security Update for libyaml (GHSA-m75h-cghq-c8h5)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

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