



CVE-2014-9130

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

Summary

CVE	CVE-2014-9130
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-08 16:59:00 UTC
Updated	2017-12-09 02:29:00 UTC
Description	scanner.c in LibYAML 0.1.5 and 0.1.6, as used in the YAML-LibYAML (aka YAML-XS) module for Perl, allows context-depe

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pyyaml	Libyaml	0.1.5	All	All	All
Application	Pyyaml	Libyaml	0.1.6	All	All	All
Application	Pyyaml	Libyaml	0.1.5	All	All	All
Application	Pyyaml	Libyaml	0.1.6	All	All	All

References

Reference	Source	Link
oss-security - Re: Re: libyaml / YAML-LibYAML DoS	MLIST	www.c
xi / libyaml / issues / #10 - Wrapped strings cause assert failure — Bitbucket	MISC	bitbuck
About Secunia Research Flexera	SECUNIA	secuni
IBM X-Force Exchange	XF	exchar
Security Advisory SA62176 - Ubuntu update for pyyaml - Secunia	SECUNIA	secuni
openSUSE-SU-2015:0319-1: moderate: Security update for perl-YAML-LibYAML	SUSE	lists.op
Security Advisory SA60944 - Perl YAML::LibYAML Module Assertion Failure Denial of Service Vulnerability - Secunia	SECUNIA	secuni
About Secunia Research Flexera	SECUNIA	secuni
xi / libyaml / commit / 2b9156756423 — Bitbucket	CONFIRM	bitbuck
USN-2461-1: LibYAML vulnerability Ubuntu	UBUNTU	www.u

openSUSE-SU-2016:1067-1: moderate: Security update for perl-YAML-LibYAML	SUSE	lists.op
Mageia Advisory: MGASA-2014-0508 - Updated yaml & perl-YAML-LibYAML packages fix CVE-2014-9130	CONFIRM	adviso
Debian -- Security Information -- DSA-3103-1 libyaml-libyaml-perl	DEBIAN	www.d
Security Advisory SA62164 - Ubuntu update for libyaml - Secunia	SECUNIA	secuni
Red Hat Customer Portal	REDHAT	rhn.rec
LibYAML and Perl YAML-LibYAML Module 'scanner.c' Remote Denial of Service Vulnerability	BID	www.s
Red Hat Customer Portal	REDHAT	rhn.rec
oss-security - libyaml / YAML-LibYAML DoS	MLIST	www.c
Security Advisory SA62774 - Red Hat update for libyaml - Secunia	SECUNIA	secuni
USN-2461-3: PyYAML vulnerability Ubuntu	UBUNTU	www.u
linux.oracle.com ELSA-2015-0100	CONFIRM	linux.o
Support / Security / Advisories // MDVSA-2015:060 Mandriva	MANDRIVA	www.n
About Secunia Research Flexera	SECUNIA	secuni
oss-security - Re: libyaml / YAML-LibYAML DoS	MLIST	www.c
Support / Security / Advisories // MDVSA-2014:242 Mandriva	MANDRIVA	www.n
USN-2461-2: libyaml-libyaml-perl vulnerability Ubuntu	UBUNTU	www.u
Debian -- Security Information -- DSA-3102-1 libyaml	DEBIAN	www.d
Red Hat Customer Portal	REDHAT	rhn.rec
CVE-2014-9130 Puppet	CONFIRM	puppe
Security Advisory SA62174 - Ubuntu update for libyaml-libyaml-perl - Secunia	SECUNIA	secuni
Debian -- Security Information -- DSA-3115-1 pyyaml	DEBIAN	www.d
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)