



# CVE-2017-5929

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

## Summary

<b>CVE</b>	CVE-2017-5929
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-13 06:59:00 UTC
<b>Updated</b>	2023-11-07 02:49:00 UTC
<b>Description</b>	QOS.ch Logback before 1.2.0 has a serialization vulnerability affecting the SocketServer and ServerSocketReceiver compo

## Risk And Classification

**Problem Types:** CWE-502

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Logback</a>	<a href="#">Logback</a>	All	All	All	All
Application	<a href="#">Qos</a>	<a href="#">Logback</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Satellite</a>	6.4	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Satellite Capsule</a>	6.4	All	All	All

## References

Reference	Source	Li
Logback News	CONFIRM	lo
Pony Mail!		lis
Pony Mail!		lis
Pony Mail!		lis
Pony Mail!		lis
Pony Mail!	MLIST	lis
Pony Mail!		lis
Red Hat Customer Portal	REDHAT	ac
Pony Mail!	MLIST	lis
Red Hat Customer Portal	REDHAT	ac

Pony Mail!	MLIST	lis
Pony Mail!	MLIST	lis
Pony Mail!		lis
Pony Mail!		lis
[cassandra-commits] 20210923 [jira] [Updated] (CASSANDRA-15829) Upgrade to logback 1.2.3 to address CVE-2017-5929		lis
Pony Mail!	MLIST	lis
Pony Mail!	MLIST	lis
Pony Mail!	MLIST	lis
Pony Mail!		lis
Pony Mail!		lis
Pony Mail!	MLIST	lis
Pony Mail!	MLIST	lis
Pony Mail!	MLIST	lis
Pony Mail!	MLIST	lis
Pony Mail!	MLIST	lis
Red Hat Customer Portal	REDHAT	ac
Pony Mail!		lis
Red Hat Customer Portal	REDHAT	ac
Pony Mail!	MLIST	lis
Pony Mail!		lis
Pony Mail!		lis
Pony Mail!		lis
Pony Mail!	MLIST	lis
Pony Mail!		lis
Pony Mail!	MLIST	lis
Pony Mail!		lis
Pony Mail!	MLIST	lis
Pony Mail!	MLIST	lis
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

980668 Java (maven) Security Update for ch.qos.logback:logback-core (GHSA-vmfg-rjjm-rjrj)

© [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](#)**