



CVE-2018-8088

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-8088
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-20 16:29:00 UTC
Updated	2023-12-27 15:15:00 UTC
Description	org.slf4j.ext.EventData in the slf4j-ext module in QOS.CH SLF4J before 1.8.0-beta2 allows remote attackers to bypass inter

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Goldengate Application Adapters	12.3.2.1.0	All	All	All
Application	Oracle	Goldengate Application Adapters	12.3.2.1.0	All	All	All
Application	Oracle	Goldengate Stream Analytics	All	All	All	All
Application	Oracle	Goldengate Stream Analytics	All	All	All	All
Application	Oracle	Utilities Framework	4.2.0.2.0	All	All	All
Application	Oracle	Utilities Framework	4.2.0.3.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.2.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.3.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.4.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.5.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.6.0	All	All	All
Application	Oracle	Utilities Framework	4.4.0.0.0	All	All	All
Application	Oracle	Utilities Framework	4.2.0.2.0	All	All	All
Application	Oracle	Utilities Framework	4.2.0.3.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.2.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.3.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.4.0	All	All	All

Application	Oracle	Utilities Framework	4.3.0.5.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.6.0	All	All	All
Application	Oracle	Utilities Framework	4.4.0.0.0	All	All	All
Application	Qos	Slf4j	All	All	All	All
Application	Qos	Slf4j	1.8.0	alpha1	All	All
Application	Qos	Slf4j	1.8.0	alpha2	All	All
Application	Qos	Slf4j	1.8.0	beta1	All	All
Application	Qos	Slf4j	1.8.0	beta2	All	All
Application	Qos	Slf4j	All	All	All	All
Application	Qos	Slf4j	1.8.0	alpha1	All	All
Application	Qos	Slf4j	1.8.0	alpha2	All	All
Application	Qos	Slf4j	1.8.0	beta1	All	All
Application	Qos	Slf4j	1.8.0	beta2	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.4.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.4.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.1	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Red Hat Customer Portal

[SLF4J-431] Mark EventData as deprecated in preparation for its removal - QOS.ch JIRA

Red Hat Customer Portal

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
SLF4J News
Red Hat Customer Portal
[SLF4J-430] Remove org.slf4j.ext.EventData due to security issue - QOS.ch JIRA
Oracle Critical Patch Update Advisory - July 2020
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Oracle Critical Patch Update Advisory - October 2020
Red Hat Customer Portal
Red Hat Customer Portal
Pony Mail!
CVE-2018-8088 SLF4j Vulnerability in NetApp Products NetApp Product Security
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Oracle Critical Patch Update Advisory - October 2021
Pony Mail!

Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Oracle Critical Patch Update Advisory - April 2019
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings
20269 IBM DB2 Multiple Vulnerabilities (6466365)
379516 IBM Sterling Secure Proxy Multiple Vulnerabilities (7142038)
87467 Oracle WebLogic Server Multiple Vulnerabilities (CPUOCT2021)

© [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](#)