



CVE-2021-28091

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

Summary

CVE	CVE-2021-28091
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-04 15:15:00 UTC
Updated	2023-11-07 03:32:00 UTC
Description	Lasso all versions prior to 2.7.0 has improper verification of a cryptographic signature.

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Entrouvert	Lasso	All	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All

References

Reference	Source	Link	Tags
lasso.git - Free software C library wich implements SAML 2.0 and Liberty Alliance standards	MISC	git.entrouvert.org	
[SECURITY] Fedora 33 Update: lasso-2.7.0-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
lasso - lasso - confirm_action	MISC	listes.entrouvert.com	
[SECURITY] [DLA 2684-1] lasso security update	MLIST	lists.debian.org	
lasso.git - Free software C library wich implements SAML 2.0 and Liberty Alliance standards	MISC	git.entrouvert.org	
[SECURITY] Fedora 33 Update: lasso-2.7.0-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
Debian -- Security Information -- DSA-4926-1 lasso	DEBIAN	www.debian.org	
[SECURITY] Fedora 34 Update: lasso-2.7.0-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 34 Update: lasso-2.7.0-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
CVE Program record	CVE ORG	www.cve.org	CONTRIB

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159324](#) Oracle Enterprise Linux Security Update for lasso (ELSA-2021-2989)

[159489](#) Oracle Enterprise Linux Security Update for lasso (ELSA-2021-4325)

[178652](#) Debian Security Update for lasso (DSA 4926-1)

[178669](#) Debian Security Update for lasso (DLA 2684-1)

[179580](#) Debian Security Update for lasso (CVE-2021-28091)

[198393](#) Ubuntu Security Notification for Lasso vulnerability (USN-4974-1)

[239529](#) Red Hat Update for lasso (RHSA-2021:2989)

[239881](#) Red Hat Update for lasso (RHSA-2021:4325)

[281621](#) Fedora Security Update for lasso (FEDORA-2021-bb3ea1e191)

[281622](#) Fedora Security Update for lasso (FEDORA-2021-508acb1153)

[296060](#) Oracle Solaris 11.4 Support Repository Update (SRU) 37.0.1.101.1 Missing (CPUJUL2021)

[316988](#) Cisco ESA, SMA,WSA Lasso SAML Implementation Vulnerability (cisco-sa-lasso-saml-jun2021-DOXNRLkD)

[316989](#) Cisco Firepower Threat Defense (FTD) Software Lasso SAML Implementation Vulnerability Affecting Cisco Products: June 2021(cisco-sa-lasso-saml-jun2021-DOXNRLkD)

[316990](#) Cisco Adaptive Security Appliance (ASA) Software Lasso SAML Implementation Vulnerability

[352394](#) Amazon Linux Security Advisory for lasso: ALAS2-2021-1660

[352806](#) Amazon Linux Security Advisory for lasso: ALAS-2021-1529

[377079](#) Alibaba Cloud Linux Security Update for lasso (ALINUX2-SA-2021:0046)

[670579](#) EulerOS Security Update for lasso (EulerOS-SA-2021-2337)

[670635](#) EulerOS Security Update for lasso (EulerOS-SA-2021-2393)

[670709](#) EulerOS Security Update for lasso (EulerOS-SA-2021-2467)

[670977](#) EulerOS Security Update for lasso (EulerOS-SA-2021-2589)

[690120](#) Free Berkeley Software Distribution (FreeBSD) Security Update for lasso (417de1e6-c31b-11eb-9633-b42e99a1b9c3)

[730129](#) Cisco Prime Collaboration Assurance Lasso SAML Implementation Vulnerability (cisco-sa-lasso-saml-jun2021-DOXNRLkD)

[750860](#) OpenSUSE Security Update for lasso (openSUSE-SU-2021-1057-1)

750000 OpenSUSE Security Update for lasso (OpenSUSE-SU-2021:1007-1)

750911 SUSE Enterprise Linux Security Update for lasso (SUSE-SU-2021:2589-1)

901752 Common Base Linux Mariner (CBL-Mariner) Security Update for lasso (7255)

904156 Common Base Linux Mariner (CBL-Mariner) Security Update for lasso (7255-1)

940121 AlmaLinux Security Update for lasso (ALSA-2021:4325)

960099 Rocky Linux Security Update for lasso (RLSA-2021:4325)

© [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](#)