



CVE-2023-1672

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

Summary

CVE	CVE-2023-1672
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-11 12:15:00 UTC
Updated	2023-11-07 21:15:00 UTC
Description	A race condition exists in the Tang server functionality for key generation and key rotation. This flaw results in a small time v

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	38	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Tang Project	Tang	All	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 3648-1] tang security update		lists.c
Fix race condition when creating/rotating keys (#123) · latchset/tang@8dbbbed1 · GitHub	MISC	github
cve-details	MISC	acce
oss-security - CVE-2023-1672: race condition in Tang exposes private keys to other processes	MISC	www.
2180999 – (CVE-2023-1672) CVE-2023-1672 tang: Race condition exists in the key generation and rotation functionality	MISC	bugzi
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[161090](#) Oracle Enterprise Linux Security Update for tang (ELSA-2023-6492)

[161159](#) Oracle Enterprise Linux Security Update for tang (ELSA-2023-7022)

[199925](#) Ubuntu Security Notification for Tang Vulnerability (USN-6489-1)

[242285](#) Red Hat Update for tang (RHSA-2023:6492)

[242422](#) Red Hat Update for tang (RHSA-2023:7022)

[284039](#) Fedora Security Update for tang (FEDORA-2023-eb9bec6e8c)

[284057](#) Fedora Security Update for tang (FEDORA-2023-3e84bba241)

[379629](#) Alibaba Cloud Linux Security Update for tang (ALINUX3-SA-2024:0043)

[6000271](#) Debian Security Update for tang (DLA 3648-1)

[907306](#) Common Base Linux Mariner (CBL-Mariner) Security Update for tang (27405-1)

[941402](#) AlmaLinux Security Update for tang (ALSA-2023:6492)

[941473](#) AlmaLinux Security Update for tang (ALSA-2023:7022)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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