CVE-2023-29409

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-29409
State	PUBLIC
Assigner	security@golang.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-02 20:15:00 UTC
Updated	2023-11-25 11:15:00 UTC
Description	Extremely large RSA keys in certificate chains can cause a client/server to expend significant CPU time verifying signatures

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	All	All	All	All
Application	Golang	Go	1.21.0	rc1	All	All
Application	Golang	Go	1.21.0	rc2	All	All
Application	Golang	Go	1.21.0	rc3	All	All

References

Reference	Source
Go: Multiple Vulnerabilities (GLSA 202311-09) — Gentoo security	
404 Not Found - Go Packages	MISC
[security] Go 1.20.7 and Go 1.19.12 are released	MISC
CVE-2023-29409 Golang Vulnerability in NetApp Products | NetApp Product Security	MISC
crypto/tls: verifying certificate chains containing large RSA keys is slow [CVE-2023-29409] · Issue #61460 · golang/go · GitHub	MISC
go.dev/cl/515257	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160998 Oracle Enterprise Linux Security Update for go-toolset and golang (ELSA-2023-5738)

161230 Oracle Enterprise Linux Security Update for podman (ELSA-2023-7765)

161231 Oracle Enterprise Linux Security Update for containernetworking-plugins (ELSA-2023-7766)

161240 Oracle Enterprise Linux Security Update for runc (ELSA-2023-7763)

161243 Oracle Enterprise Linux Security Update for skopeo (ELSA-2023-7762)

161244 Oracle Enterprise Linux Security Update for buildah (ELSA-2023-7764)

161289 Oracle Enterprise Linux Security Update for container-tools:4.0 (ELSA-2024-0121)

242176 Red Hat Update for go-toolset and golang (RHSA-2023:5738)

242228 Red Hat Update for OpenStack Platform 17.1.1 (RHSA-2023:5969)

242365 Red Hat Update for OpenStack Platform 16.2.5 (RHSA-2023:5964)

242381 Red Hat Update for OpenStack Platform 16.2.5 (RHSA-2023:5965)

242464 Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:6840)

242569 Red Hat Update for podman (RHSA-2023:7765)

242584 Red Hat Update for runc (RHSA-2023:7763)

242585 Red Hat Update for containernetworking-plugins (RHSA-2023:7766)

242587 Red Hat Update for buildah (RHSA-2023:7764)

242593 Red Hat Update for skopeo (RHSA-2023:7762)

242736 Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2024:0292)

242737 Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2024:0293)

242882 Red Hat Update for container-tools:4.0 (RHSA-2024:0121)

296103 Oracle Solaris 11.4 Support Repository Update (SRU) 61.151.2 Missing (CPUJUL2023)

355840 Amazon Linux Security Advisory for runc : ALAS2NITRO-ENCLAVES-2023-027

355842 Amazon Linux Security Advisory for cni-plugins : ALAS2-2023-2208

355843 Amazon Linux Security Advisory for nerdctl : ALAS2-2023-2210

355852 Amazon Linux Security Advisory for golang : ALAS2-2023-2211

355856 Amazon Linux Security Advisory for containerd : ALAS2NITRO-ENCLAVES-2023-028

355857 Amazon Linux Security Advisory for amazon-cloudwatch-agent : ALAS2-2023-2209

355859 Amazon Linux Security Advisory for runc : ALAS2DOCKER-2023-026

355866 Amazon Linux Security Advisory for containerd : ALAS2DOCKER-2023-027

355868 Amazon Linux Security Advisory for nerdctl : ALAS2023-2023-309

355876 Amazon Linux Security Advisory for amazon-cloudwatch-agent : ALAS2023-2023-307

355880 Amazon Linux Security Advisory for containerd : ALAS2023-2023-308

356112 Amazon Linux Security Advisory for docker : ALAS2023-2023-345

356115 Amazon Linux Security Advisory for amazon-ecr-credential-helper : ALAS2023-2023-346

356344 Amazon Linux Security Advisory for golang : AL2012-2023-447

356362 Amazon Linux Security Advisory for golang : ALAS-2023-1848

356363 Amazon Linux Security Advisory for containerd : ALAS-2023-1849

356374 Amazon Linux Security Advisory for amazon-ssm-agent : ALAS2023-2023-373

356428 Amazon Linux Security Advisory for amazon-ssm-agent : ALAS2-2023-2303

356565 Amazon Linux Security Advisory for containerd : ALAS2ECS-2023-008

503191 Alpine Linux Security Update for go

506085 Alpine Linux Security Update for go

673336 EulerOS Security Update for golang (EulerOS-SA-2023-3006)

673747 EulerOS Security Update for golang (EulerOS-SA-2023-3178)

673755 EulerOS Security Update for golang (EulerOS-SA-2023-2877)

673850 EulerOS Security Update for golang (EulerOS-SA-2024-1140)

673911 EulerOS Security Update for golang (EulerOS-SA-2023-2896)

673945 EulerOS Security Update for golang (EulerOS-SA-2023-3213)

674001 EulerOS Security Update for golang (EulerOS-SA-2023-3029)

710791 Gentoo Linux Go Multiple Vulnerabilities (GLSA 202311-09)

754270 SUSE Enterprise Linux Security Update for go1.19 (SUSE-SU-2023:3263-1)

754950 SUSE Enterprise Linux Security Update for go1.19-openssl (SUSE-SU-2023:3841-1)

754951 SUSE Enterprise Linux Security Update for go1.20-openssl (SUSE-SU-2023:3840-1)

754977 SUSE Enterprise Linux Security Update for grafana (SUSE-SU-2023:3886-1)

754978 SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2023:3868-1)

754979 SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2023:3867-1)

754988 SUSE Enterprise Linux Security Update for Golang Prometheus (SUSE-SU-2023:3888-1)

755293 SUSE Enterprise Linux Maintenance update for SUSE Manager 4.3.8 Release Notes (SUSE-SU-2023:3885-1)

770214 Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:6840)

770224 Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2024:0293)

907881 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (27812-2)

907924 Common Base Linux Mariner (CBL-Mariner) Security Update for msft-golang (27814-1)

941298 AlmaLinux Security Update for go-toolset and golang (ALSA-2023:5738)

941495 AlmaLinux Security Update for podman (ALSA-2023:7765)

941497 AlmaLinux Security Update for runc (ALSA-2023:7763)

941498 AlmaLinux Security Update for containernetworking-plugins (ALSA-2023:7766)

941499 AlmaLinux Security Update for skopeo (ALSA-2023:7762)

941500 AlmaLinux Security Update for buildah (ALSA-2023:7764)

941535 AlmaLinux Security Update for container-tools:4.0 (ALSA-2024:0121)

961058 Rocky Linux Security Update for go-toolset and golang (RLSA-2023:5738)

© 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 registred 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**