CVE-2021-34558

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-34558
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-15 14:15:00 UTC
Updated	2023-11-07 03:36:00 UTC
Description	The crypto/tls package of Go through 1.16.5 does not properly assert that the type of public key in an X.509 certificate matc

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Golang	Go	All	All	All	All
Application	Golang	Go	All	All	All	All
Application	Netapp	Cloud Insights Telegraf	-	All	All	All
Application	Netapp	Storagegrid	-	All	All	All
Application	Netapp	Trident	-	All	All	All
Application	Oracle	Timesten In-memory Database	All	All	All	All

References

Reference	Source	Lir
[SECURITY] Fedora 33 Update: buildah-1.21.4-5.fc33 - package-announce - Fedora Mailing-Lists		list
[SECURITY] Fedora 34 Update: buildah-1.21.4-5.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	list
[SECURITY] Fedora 33 Update: podman-3.2.3-2.fc33 - package-announce - Fedora Mailing-Lists		list
[SECURITY] Fedora 33 Update: buildah-1.21.4-5.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	list
[SECURITY] Fedora 34 Update: golang-1.16.6-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	list
[SECURITY] Fedora 34 Update: podman-3.2.3-2.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	list

Oracle Critical Patch Update Advisory - October 2021	MISC	ww
Release History - The Go Programming Language	MISC	gol
[SECURITY] Fedora 33 Update: containernetworking-plugins-1.0.0-0.3.rc1.fc33 - package-announce - Fedora Mailing-Lists		list
[SECURITY] Fedora 33 Update: golang-1.15.14-1.fc33 - package-announce - Fedora Mailing-Lists		list
Oracle Critical Patch Update Advisory - January 2022	MISC	ww
[SECURITY] Fedora 34 Update: containernetworking-plugins-1.0.0-0.3.rc1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	list
CVE-2021-34558 Golang Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	sec
[SECURITY] Fedora 34 Update: buildah-1.21.4-5.fc34 - package-announce - Fedora Mailing-Lists		list
[SECURITY] Fedora 34 Update: podman-3.2.3-2.fc34 - package-announce - Fedora Mailing-Lists		list
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	sec
[SECURITY] Fedora 34 Update: containernetworking-plugins-1.0.0-0.3.rc1.fc34 - package-announce - Fedora Mailing-Lists		list
[SECURITY] Fedora 33 Update: podman-3.2.3-2.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	list
[SECURITY] Fedora 33 Update: containernetworking-plugins-1.0.0-0.3.rc1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	list
[SECURITY] Fedora 34 Update: grafana-7.5.10-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	list
[security] Go 1.16.6 and Go 1.15.14 are released	MISC	gro
[SECURITY] Fedora 33 Update: golang-1.15.14-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	list
[SECURITY] Fedora 34 Update: grafana-7.5.10-1.fc34 - package-announce - Fedora Mailing-Lists		list
golang-announce - Google Groups	MISC	gro
[SECURITY] Fedora 34 Update: golang-1.16.6-1.fc34 - package-announce - Fedora Mailing-Lists		list
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159347 Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2021-3076)
- 159473 Oracle Enterprise Linux Security Update for grafana (ELSA-2021-4226)
- 160293 Oracle Enterprise Linux Security Update for podman (ELSA-2022-7954)
- 179916 Debian Security Update for golang-1.15 (CVE-2021-34558)
- 239537 Red Hat Update for OpenShift Container Platform 4.8.4 (RHSA-2021:2984)
- 239549 Red Hat Update for go-toolset:rhel8 (RHSA-2021:3076)
- 239555 Red Hat Update for OpenShift Container Platform 4.6.42 (RHSA-2021:3009)
- 239606 Red Hat Update for OpenShift Container Platform 4.8.9 packages (RHSA-2021:3248)

239694 Red Hat Update for OpenShift Container Platform 4.8.15 packages and (RHSA-2021:3820)

239800 Red Hat Update for grafana security (RHSA-2021:4226)

240023 Red Hat Update for OpenStack Platform 16.2 (RHSA-2022:0237)

240030 Red Hat Update for OpenStack Platform 16.1 (RHSA-2022:0260)

240171 Red Hat Update for OpenStack Platform 16.1 (RHSA-2022:0988)

240173 Red Hat Update for OpenStack Platform 16.2 (RHSA-2022:0998)

240876 Red Hat Update for podman (RHSA-2022:7954)

281745 Fedora Security Update for golang (FEDORA-2021-1bfb61f77c)

281746 Fedora Security Update for golang (FEDORA-2021-25c0011e78)

281772 Fedora Security Update for podman (FEDORA-2021-3a55403080)

281773 Fedora Security Update for buildah (FEDORA-2021-47d259d3cf)

281781 Fedora Security Update for podman (FEDORA-2021-6ac9b98f9e)

281782 Fedora Security Update for buildah (FEDORA-2021-ffa749f7f7)

281783 Fedora Security Update for containernetworking (FEDORA-2021-54f88bebd4)

281784 Fedora Security Update for containernetworking (FEDORA-2021-07e4d20196)

281970 Fedora Security Update for grafana (FEDORA-2021-c35235c250)

296063 Oracle Solaris 11.4 Support Repository Update (SRU) 45.119.2 Missing (CPUAPR2022)

352505 Amazon Linux Security Advisory for golang: ALAS2-2021-1694

352808 Amazon Linux Security Advisory for golang: ALAS-2021-1527

352827 Amazon Linux Security Advisory for golang: AL2012-2021-351

375835 Go Lang Transport Layer Security (TLS) Clients Vulnerability

377560 Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2021:0060)

378883 Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)

501571 Alpine Linux Security Update for go

501860 Alpine Linux Security Update for go

670823 EulerOS Security Update for golang (EulerOS-SA-2021-2710)

670953 EulerOS Security Update for golang (EulerOS-SA-2021-2685)

671161 EulerOS Security Update for golang (EulerOS-SA-2021-2802)

671187 EulerOS Security Update for golang (EulerOS-SA-2021-2930)

690088 Free Berkeley Software Distribution (FreeBSD) Security Update for go (c365536d-e3cf-11eb-9d8d-b37b683944c2)

710584 Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)

750861 OpenSUSE Security Update for go1.15 (openSUSE-SU-2021:2398-1)

750863 OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:2392-1)

750881 OpenSUSE Security Update for go1.15 (openSUSE-SU-2021:1079-1)

750884 OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:1078-1)

770069 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:3009)

770070 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:2984)

770078 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:3248)

770082 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:3820)

770090 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-3820)

770102 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-3248)

770106 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-2984)

770119 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021-3009)

900203 CBL-Mariner Linux Security Update for golang 1.15.13

903464 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (4744)

907766 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (4744-1)

940047 AlmaLinux Security Update for grafana (ALSA-2021:4226)

940126 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2021:3076)

940834 AlmaLinux Security Update for podman (ALSA-2022:7954)

960708 Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2021:3076)

960842 Rocky Linux Security Update for grafana (RLSA-2021:4226)