CVE-2022-28327

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-28327
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-20 10:15:00 UTC
Updated	2023-11-07 03:45:00 UTC
Description	The generic P-256 feature in crypto/elliptic in Go before 1.17.9 and 1.18.x before 1.18.1 allows a panic via long scalar input

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedoraproject	Extra Packages For Enterprise Linux	7.0	All	All	All
Application	Fedoraproject	Extra Packages For Enterprise Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Golang	Go	All	All	All	All

References

Reference	Source	L
April 2022 Golang Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	s
[security] Go 1.18.1 and Go 1.17.9 are released	CONFIRM	g
[SECURITY] Fedora 36 Update: golang-github-chromedp-0.8.1-2.fc36 - package-announce - Fedora Mailing-Lists		li
[SECURITY] Fedora 36 Update: golang-github-lucas-clemente-quic-0.27.2-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	li
[SECURITY] Fedora 34 Update: clash-1.6.5-2.fc34 - package-announce - Fedora Mailing-Lists		li
[SECURITY] Fedora 34 Update: gron-0.6.1-2.fc34 - package-announce - Fedora Mailing-Lists		li
[SECURITY] Fedora 36 Update: aquatone-1.7.0-7.fc36 - package-announce - Fedora Mailing-Lists		li
[SECURITY] Fedora 34 Update: gron-0.6.1-2.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	li

cert-portal.siemens.com/productcert/pdf/ssa-744259.pdf	MISC	c
[SECURITY] Fedora 35 Update: golang-1.16.15-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	li
[SECURITY] Fedora 36 Update: golang-github-chromedp-0.8.1-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	li
[SECURITY] Fedora 35 Update: golang-1.16.15-2.fc35 - package-announce - Fedora Mailing-Lists		li
[SECURITY] Fedora 34 Update: clash-1.6.5-2.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	li
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	s
[SECURITY] Fedora 36 Update: aquatone-1.7.0-7.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	li
[SECURITY] Fedora 35 Update: fzf-0.29.0-2.fc35 - package-announce - Fedora Mailing-Lists		li
[SECURITY] Fedora 36 Update: golang-github-lucas-clemente-quic-0.27.2-1.fc36 - package-announce - Fedora Mailing-Lists		li
[SECURITY] Fedora 35 Update: fzf-0.29.0-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	li
golang-announce - Google Groups	MISC	g
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159885 Oracle Enterprise Linux Security Update for go-toolset:ol8addon (ELSA-2022-14844)
- 159959 Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2022-5337)
- 159981 Oracle Enterprise Linux Security Update for go-toolset:ol8addon (ELSA-2022-17956)
- 240503 Red Hat Update for go-toolset:rhel8 (RHSA-2022:5337)
- 240607 Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2022:5068)
- 240616 Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:6094)
- 241776 Red Hat Update for red hat openshift enterprise (RHSA-2023:3914)
- 282790 Fedora Security Update for clash (FEDORA-2022-a49babed75)
- 282801 Fedora Security Update for gron (FEDORA-2022-53f0c619c5)
- 282878 Fedora Security Update for golang (FEDORA-2022-c0f780ecf1)
- 282887 Fedora Security Update for golang (FEDORA-2022-e46e6e8317)
- 282893 Fedora Security Update for 3mux (FEDORA-2022-fae3ecee19)
- 282931 Fedora Security Update for apptainer (FEDORA-2022-ba365d3703)
- 282947 Fedora Security Update for 3mux (FEDORA-2022-3969b64d4b)
- 283049 Fedora Security Update for fzf (FEDORA-2022-30c5ed5625)

284299 Fedora Security Update for etcd (FEDORA-2022-28d38313c8)

354041 Amazon Linux Security Advisory for golang : ALAS2-2022-1830

354064 Amazon Linux Security Advisory for golist : ALAS2-2022-1847

354067 Amazon Linux Security Advisory for golang : ALAS2-2022-1846

354069 Amazon Linux Security Advisory for golang : ALAS-2022-1635

354083 Amazon Linux Security Advisory for runc : ALAS2DOCKER-2022-020

354088 Amazon Linux Security Advisory for golang-github-syndtr-gocapability : ALAS2-2022-1865

354089 Amazon Linux Security Advisory for golang-googlecode-sqlite : ALAS2-2022-1862

354090 Amazon Linux Security Advisory for golang-github-kr-pty : ALAS2-2022-1864

354091 Amazon Linux Security Advisory for go-rpm-macros : ALAS2-2022-1863

354092 Amazon Linux Security Advisory for golang-googlecode-net : ALAS2-2022-1861

354093 Amazon Linux Security Advisory for golang-github-gorilla-mux : ALAS2-2022-1860

354094 Amazon Linux Security Advisory for golang-github-gorilla-context : ALAS2-2022-1859

354096 Amazon Linux Security Advisory for golang-github-godbus-dbus : ALAS2-2022-1858

354370 Amazon Linux Security Advisory for golang-github-cpuguy83-md2man : ALAS2022-2022-140

354493 Amazon Linux Security Advisory for golist : ALAS2022-2022-133

354504 Amazon Linux Security Advisory for golist : ALAS2022-2022-192

354527 Amazon Linux Security Advisory for golang : ALAS2022-2022-193

354566 Amazon Linux Security Advisory for golang : ALAS-2022-193

355111 Amazon Linux Security Advisory for golist : ALAS2023-2023-046

355186 Amazon Linux Security Advisory for golang-github-cpuguy83-md2man : ALAS2023-2023-047

355212 Amazon Linux Security Advisory for golang : ALAS2023-2023-048

356304 Amazon Linux Security Advisory for golang : ALASGOLANG1.19-2023-002

377375 Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2022:0131)

378599 Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)

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

502300 Alpine Linux Security Update for go

671844 EulerOS Security Update for golang (EulerOS-SA-2022-1890)

671868 EulerOS Security Update for golang (EulerOS-SA-2022-1930)

671921 EulerOS Security Update for golang (EulerOS-SA-2022-1966)

671962 EulerOS Security Update for golang (EulerOS-SA-2022-1996)

671976 EulerOS Security Update for golang (EulerOS-SA-2022-2157)

671990 EulerOS Security Update for golang (EulerOS-SA-2022-2132)

672245 EulerOS Security Update for golang (EulerOS-SA-2022-2610)

690861 Free Berkeley Software Distribution (FreeBSD) Security Update for go (61bce714-ca0c-11ec-9cfc-10c37b4ac2ea)

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

753094 SUSE Enterprise Linux Security Update for go1.18 (SUSE-SU-2022:1410-1)

753236 SUSE Enterprise Linux Security Update for go1.17 (SUSE-SU-2022:1411-1)

754047 SUSE Enterprise Linux Security Update for go1.18-openssl (SUSE-SU-2023:2312-1)

770161 Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:5068)

770162 Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:6094)

770204 Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2023:3914)

900864 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9546)

901558 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9547)

902190 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9546-1)

902274 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9547-1)

907751 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9546-2)

907812 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9547-2)

960300 Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2022:5337)

960612 Rocky Linux Security Update for go-toolset and golang (RLSA-2022:5799)