CVE-2021-3114

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3114
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-26 18:16:00 UTC
Updated	2023-11-07 03:37:00 UTC
Description	In Go before 1.14.14 and 1.15.x before 1.15.7, crypto/elliptic/p224.go can generate incorrect outputs, related to an underflo

Risk And Classification

Problem Types: CWE-682

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
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Golang	Go	All	All	All	All
Application	Golang	Go	All	All	All	All
Application	Netapp	Cloud Insights Telegraf Agent	-	All	All	All
Application	Netapp	Cloud Insights Telegraf Agent	-	All	All	All
Application	Netapp	Storagegrid	-	All	All	All
Application	Netapp	Storagegrid	-	All	All	All

References

Reference	Source	Link	Tag
[SECURITY] [DLA 2591-1] golang-1.7 security update	MLIST	lists.debian.org	Mail
Debian -- Security Information -- DSA-4848-1 golang-1.11	DEBIAN	www.debian.org	Third
crypto/elliptic: fix P-224 field reduction · golang/go@d95ca91 · GitHub	CONFIRM	github.com	Patc

[security] Go 1.15.7 and Go 1.14.14 are released	CONFIRM	groups.google.com	Rele
[SECURITY] Fedora 33 Update: golang-1.15.7-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Thir
[SECURITY] [DLA 2592-1] golang-1.8 security update	MLIST	lists.debian.org	Mail
February 2021 Golang Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Thir
[SECURITY] Fedora 33 Update: golang-1.15.7-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159209 Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2021-1746)
- 159473 Oracle Enterprise Linux Security Update for grafana (ELSA-2021-4226)
- 179945 Debian Security Update for golang-1.15 (CVE-2021-3114)
- 239197 Red Hat Update for OpenShift Container Platform 4.7.4 (RHSA-2021:0958)
- 239272 Red Hat Update for OpenShift Container Platform 4.7.9 packages and (RHSA-2021:1366)
- 239312 Red Hat Update for go-toolset:rhel8 (RHSA-2021:1746)
- 239359 Red Hat Update for OpenShift Container Platform 4.7.11 (RHSA-2021:1551)
- 239525 Red Hat Update for OpenShift Container Platform 4.8.2 (RHSA-2021:2437)
- 239800 Red Hat Update for grafana security (RHSA-2021:4226)
- 240042 Red Hat Update for openshift container storage 3.11.z (RHSA-2022:0308)
- 352297 Amazon Linux Security Update for golang: AL2012-2021-340
- 501575 Alpine Linux Security Update for go
- 670323 EulerOS Security Update for golang (EulerOS-SA-2021-1901)
- 670350 EulerOS Security Update for golang (EulerOS-SA-2021-1874)
- 670378 EulerOS Security Update for golang (EulerOS-SA-2021-1947)
- 670399 EulerOS Security Update for golang (EulerOS-SA-2021-1926)
- 670893 EulerOS Security Update for golang (EulerOS-SA-2021-1901)
- 690411 Free Berkeley Software Distribution (FreeBSD) Security Update for go (6a4805d5-5aaf-11eb-a21d-79f5bc5ef6a9)
- 710584 Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)

750384 OpenSUSE Security Update for go1.14 (openSUSE-SU-2021:0194-1)

750385 OpenSUSE Security Update for go1.14 (openSUSE-SU-2021:0190-1)

750387 OpenSUSE Security Update for go1.15 (openSUSE-SU-2021:0192-1)

770054 Red Hat OpenShift Container Platform 4.7.4 Security Update (RHSA-2021:0958)

770055 Red Hat OpenShift Container Platform 4.7.5 Security and Bug Fix Update (RHSA-2021:1006)

770058 Red Hat OpenShift Container Platform 4.7.9 Packages and Security Update (RHSA-2021:1366)

770059 Red Hat OpenShift Container Platform 4.7.11 Security and Bug Fix Update (RHSA-2021:1551)

770074 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:2437)

770091 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-1366)

770109 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-1006)

770111 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-2437)

770112 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-1551)

770121 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-0958)

900206 CBL-Mariner Linux Security Update for golang 1.15.5

903480 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (3832)

907747 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (3832-1)

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

940200 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2021:1746)

960773 Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2021:1746)

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