Security Export

Wed Aug 24, 2022

Exported by: muhammad.mujtaba

Package type: Docker

Component name: ccss:4.1.0-gl1200247

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Malicious package monorepo-symlink-test for Node.js		Critical	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/resolve/package.json/test/resolver/multirepo/package.json	monorepo-symlink-test	All Versions		2022-07-27T07:41:13Z
A too-short encoded message can cause a panic in Float.GobDecode and Rat GobDecode in math/big in Go before 1.17.13 and 1.18.5, potentially allowing a denial of service.	CVE-2022-32189	High	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.13,1.18.0 <= Version < 1.18.5	1.17.13,1.18.5	2022-08-23T07:41:41Z
Uncontrolled recursion in Unmarshal in encoding/xml before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via unmarshalling an XML document into a Go struct which has a nested field that uses the 'any' field tag.	CVE-2022-30633	High	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.12,1.18.0 <= Version < 1.18.4	1.17.12,1.18.4	2022-08-23T07:41:41Z

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Code injection in Cmd.Start in os/exec before Go 1.17.11 and Go 1.18.3 allows execution of any binaries in the working directory named either "..com" or "..exe" by calling Cmd.Run, Cmd.Start, Cmd.Output, or Cmd.CombinedOutput when Cmd.Path is unset.	CVE-2022-30580	High	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.11,1.18.0 <= Version < 1.18.3	1.17.11,1.18.3	2022-08-23T07:41:37Z
Uncontrolled recursion in Decoder.Skip in encoding/xml before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a deeply nested XML document.	CVE-2022-28131	High	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.12,1.18.0 <= Version < 1.18.4	1.17.12,1.18.4	2022-08-23T07:41:41Z
Uncontrolled recursion in Reader.Read in compress/gzip before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via an archive containing a large number of concatenated 0-length compressed files.	CVE-2022-30631	High	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.12,1.18.0 <= Version < 1.18.4	1.17.12,1.18.4	2022-08-23T07:41:37Z
Uncontrolled recursion in Glob in io/fs before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a path which contains a large number of path separators.	CVE-2022-30630	High	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.12,1.18.0 <= Version < 1.18.4	1.17.12,1.18.4	2022-08-23T07:41:41Z
Infinite loop in Read in crypto/rand before Go 1.17.11 and Go 1.18.3 on Windows allows attacker to cause an indefinite hang by passing a buffer larger than 1 << 32 - 1 bytes.	CVE-2022-30634	High	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.11	1.17.11,1.18.3	2022-07-24T07:41:43Z

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Incorrect conversion of certain invalid paths to valid, absolute paths in Clean in path/filepath before Go 1.17.11 and Go 1.18.3 on Windows allows potential directory traversal attack.	CVE-2022-29804	High	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.11,1.18.0 <= Version < 1.18.3	1.17.11,1.18.3	2022-08-23T07:41:42Z
Uncontrolled recursion in Decoder.Decode in encoding/gob before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a message which contains deeply nested structures.	CVE-2022-30635	High	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.12,1.18.0 <= Version < 1.18.4	1.17.12,1.18.4	2022-08-23T07:41:42Z
Uncontrolled recursion in Glob in path/filepath before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a path containing a large number of path separators.	CVE-2022-30632	High	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.12,1.18.0 <= Version < 1.18.4	1.17.12,1.18.4	2022-08-23T07:41:37Z
Improper exposure of client IP addresses in net/http before Go 1.17.12 and Go 1.18.4 can be triggered by calling httputil.ReverseProxy.ServeHTTP with a Request.Header map containing a nil value for the X-Forwarded-For header, which causes ReverseProxy to set the client IP as the value of the X-Forwarded-For header.	CVE-2022-32148	Medium	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.12,1.18.0 <= Version < 1.18.4	1.17.12,1.18.4	2022-08-23T07:41:42Z
Acceptance of some invalid Transfer-Encoding headers in the HTTP/1 client in net/http before Go 1.17.12 and Go 1.18.4 allows HTTP request smuggling if combined with an intermediate server that also improperly fails to reject the header as invalid.	CVE-2022-1705	Medium	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.12,1.18.0 <= Version < 1.18.4	1.17.12,1.18.4	2022-08-23T07:41:41Z

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Go before 1.17.10 and 1.18.x before 1.18.2 has Incorrect Privilege Assignment. When called with a non-zero flags parameter, the Faccessat function could incorrectly report that a file is accessible.	CVE-2022-29526	Medium	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.10,1.18.0 <= Version < 1.18.2	1.17.10,1.18.2	2022-07-02T07:43:05Z
Uncontrolled recursion in the Parse functions in go/parser before Go 1.17.12 and Go 1.18.4 allow an attacker to cause a panic due to stack exhaustion via deeply nested types or declarations.	CVE-2022-1962	Medium	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.12,1.18.0 <= Version < 1.18.4	1.17.12,1.18.4	2022-08-23T07:41:42Z
Go Cryptography acme/autocert/cache.go Get() Function Path Traversal File Disclosure Weakness	CVE-2022-30636	Low	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	<= 1.18.3		2022-06-07T07:41:14Z
Non-random values for ticket_age_add in session tickets in crypto/tls before Go 1.17.11 and Go 1.18.3 allow an attacker that can observe TLS handshakes to correlate successive connections by comparing ticket ages during session resumption.	CVE-2022-30629	Low	sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/azcopy-linux/azcopy_linux_amd64/github.com/lang/go/go; sha256__1e2f7d8a9eb4bb82dd935cf271521a49da25be1d6480eeb15092702be1407837.tar.gz/usr/local/Nuance/ccss/node_modules/@azure-tools/azcopy-linux/package.json/dist/bin/azcopy_linux_amd64/github.com/lang/go/go	github.com/golang/go	< 1.17.11,1.18.0 <= Version < 1.18.3	1.17.11,1.18.3	2022-08-23T07:41:42Z