GoLang	CVE	description
jwt-go v3.2.0+incompatible	CVE-2020-26160	jwt-go before 4.0.0-preview1 allows attackers to bypass intended access restrictions in situations with []string{} for m["aud"] (which is allowed by the specification). Because the type assertion fails, "" is the value of aud. This is a security problem if the JWT token is presented to a service that lacks its own audience check.
Angular		
glob-parent v5.1.2	CVE-2020-28469	This affects the package glob-parent before 5.1.2. The enclosure regex used to check for strings ending in enclosure containing path separator.
node-forge v0.10.0	CVE-2022-24773	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.3.0, RSA PKCS#1 v1.5 signature verification code does not properly check `DigestInfo` for a proper ASN.1 structure. This can lead to successful verification with signatures that contain invalid structures but a valid digest. The issue has been addressed in `node-forge` version 1.3.0. There are currently no known workarounds.