CVE Mitigations from V2.2.5 to V2.6.9			

Image	Tag	CVE	Mitigation
Image: cf-debugger Count: 3			
cf-debugger	1.3.7	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-debugger	1.3.7	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-debugger	1.3.7	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: cf-deploy-kubernetes Count: 4			
cf-deploy-kubernetes	16.2.6	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-deploy-kubernetes	16.2.6	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-deploy-kubernetes	16.2.6	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-deploy-kubernetes	16.2.6	CVE-2022-28391	We do not use DNS PTR records in any part of our resources or applications. DNS PTR records are used to reverse IP address mapping to domain names, which are often used in the network environment to identify devices. Since our service does not depend on this mechanism and does not use netstat for any operations or processes, the vulnerability related to the manipulation of PTR records through the netstat utility cannot have any effect.
Image: cf-docker-builder			
cf-docker-builder	1.4.4	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
cf-docker-builder	1.4.4	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-builder	1.4.4	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-builder	1.4.4	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-builder	1.4.4	CVE-2022-30065	We do not use DNS PTR records in any part of our resources or applications. DNS PTR records are used to reverse IP address mapping to domain names, which are often used in the network environment to identify devices. Since our service does not depend on this mechanism and does not use netstat for any operations or processes, the vulnerability related to the manipulation of PTR records through the netstat utility cannot have any effect.
cf-docker-builder	1.4.4	CVE-2022-28391	
Image: cf-docker-puller Count: 4			
cf-docker-puller	8.0.20	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly

CVE Mitigations from V2.2.5 to V2.6.9			

Image	Tag	CVE	Mitigation
cf-docker-puller	8.0.20	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-puller	8.0.20	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-puller	8.0.20	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: cf-docker-pusher			
cf-docker-pusher	6.0.17	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-pusher	6.0.17	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-pusher	6.0.17	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-pusher	6.0.17	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
Image: cf-docker-tag-pusher Count: 4			
cf-docker-tag-pusher	1.3.15	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-tag-pusher	1.3.15	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-tag-pusher	1.3.15	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-tag-pusher	1.3.15	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
Image: cf-git-cloner Count: 6			
cf-git-cloner	10.2.0	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-git-cloner	10.2.0	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-git-cloner	10.2.0	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-git-cloner	10.2.0	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-git-cloner	10.2.0	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly

CVE Mitigations from V2.2.5 to V2.6.9			

Image	Tag	CVE	Mitigation
cf-git-cloner	10.2.0	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: chartmuseum Count: 4			
chartmuseum	8795e993	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
chartmuseum	8795e993	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
chartmuseum	8795e993	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
chartmuseum	8795e993	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: docker.io/bitnami/consul Count: 1			
docker.io/bitnami/consul	1.21.0-debian-12-r1	PRISMA-2023-0056	Latest upstream version
Image: engine Count: 5			
engine	1.177.7	CVE-2024-29415	This package is not used inside our business logic to validate the loopback addresses thus we are not affected by this vulnerability.
engine	1.177.7	CVE-2024-11023	Firebase JavaScript SDK utilizes a "FIREBASE_DEFAULTS" cookie to store configuration data, including an "_authTokenSyncURL" field for session synchronization. If this cookie field is preset via an attacker by any other method, the attacker can manipulate the "_authTokenSyncURL" to point to their own server and it would allow am actor to capture user session data transmitted by the SDK. As it stems from the description, this issue affects only browser usage of Firebase SDK, and not relevant for server-side JS because of absence of cookies per se.
engine	1.177.7	CVE-2022-33987	dependency is located in "npm" and not related/used to app package/run.
engine	1.177.7	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.
engine	1.177.7	CVE-2024-28176	Service utilizes the jose module as nested module in jsonwebtoket. But does not perform any operation of unpacking decrypted text, and we don't use JWE at all. This vulnerability will not impact our service
Image: pikolo Count: 5			
pikolo	0.14.3	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
pikolo	0.14.3	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
pikolo	0.14.3	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.

CVE Mitigations from V2.2.5 to V2.6.9			

Image	Tag	CVE	Mitigation
pikolo	0.14.3	CVE-2022-28391	We do not use DNS PTR records in any part of our resources or applications. DNS PTR records are used to reverse IP address mapping to domain names, which are often used in the network environment to identify devices. Since our service does not depend on this mechanism and does not use netstat for any operations or processes, the vulnerability related to the manipulation of PTR records through the netstat utility cannot have any effect.
pikolo	0.14.3	CVE-2022-30065	cf-docker-builder
Image: quay.io/codefresh/cf-debugger Count: 1			
quay.io/codefresh/cf-debugger	1.3.7	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
Image: quay.io/codefresh/cf-git-cloner			
quay.io/codefresh/cf-git-cloner	10.2.0	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
Image: quay.io/codefresh/chartmuseum Count: 1			
quay.io/codefresh/chartmuseum	8795e993	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: quay.io/codefresh/pikolo Count: 1			
quay.io/codefresh/pikolo	0.14.3	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-abac Count: 5			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-abac	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-abac	1.3344.0-onprem-5c8af92	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-abac	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-abac	1.3344.0-onprem-5c8af92	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-abac	1.3344.0-onprem-5c8af92	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-analytics-reporter Count: 5			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-analytics-reporter	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-analytics-reporter	1.3344.0-onprem-5c8af92	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-analytics-reporter	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly

CVE Mitigations from V2.2.5 to V2.6.9			

Image	Tag	CVE	Mitigation
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-analytics-reporter	1.3344.0-onprem-5c8af92	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-analytics-reporter	1.3344.0-onprem-5c8af92	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-events Count: 5			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-events	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-events	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-events	1.3344.0-onprem-5c8af92	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-events	1.3344.0-onprem-5c8af92	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-events	1.3344.0-onprem-5c8af92	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-graphql Count: 6			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-graphql	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-graphql	1.3344.0-onprem-5c8af92	CVE-2024-29415	This package is not used inside our business logic to validate the loopback addresses thus we are not affected by this vulnerability.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-graphql	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-graphql	1.3344.0-onprem-5c8af92	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-graphql	1.3344.0-onprem-5c8af92	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-api-graphql	1.3344.0-onprem-5c8af92	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-audit Count: 5			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-audit	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-audit	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-audit	1.3344.0-onprem-5c8af92	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.

[CVE Mitigations from V2.2.5 to V2.6.9]

Image	Tag	CVE	Mitigation
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-audit	1.3344.0-onprem-5c8af92	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-audit	1.3344.0-onprem-5c8af92	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-broadcaster Count: 6			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-broadcaster	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-broadcaster	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-broadcaster	1.3344.0-onprem-5c8af92	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-broadcaster	1.3344.0-onprem-5c8af92	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-broadcaster	1.3344.0-onprem-5c8af92	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-broadcaster	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-cron-executor Count: 5			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-cron-executor	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-cron-executor	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-cron-executor	1.3344.0-onprem-5c8af92	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-cron-executor	1.3344.0-onprem-5c8af92	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-cron-executor	1.3344.0-onprem-5c8af92	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-event-handler			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-event-handler	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-event-handler	1.3344.0-onprem-5c8af92	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-event-handler	1.3344.0-onprem-5c8af92	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-event-handler	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly

CVE Mitigations from V2.2.5 to V2.6.9			

Image	Tag	CVE	Mitigation
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-event-handler	1.3344.0-onprem-5c8af92	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-promotion-orchestrator Count: 7			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-promotion-orchestrator	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-promotion-orchestrator	1.3344.0-onprem-5c8af92	CVE-2024-29415	This package is not used inside our business logic to validate the loopback addresses thus we are not affected by this vulnerability.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-promotion-orchestrator	1.3344.0-onprem-5c8af92	CVE-2023-26108	Vulnerability is related to StreamableFile api -- we are not using this api to return files. Also, we do not allow to download files from our services.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-promotion-orchestrator	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-promotion-orchestrator	1.3344.0-onprem-5c8af92	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-promotion-orchestrator	1.3344.0-onprem-5c8af92	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-promotion-orchestrator	1.3344.0-onprem-5c8af92	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-ui Count: 4			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-ui	1.3344.0-onprem-5c8af92	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-ui	1.3344.0-onprem-5c8af92	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-ui	1.3344.0-onprem-5c8af92	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh-io/argo-platform-ui	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/cf-broadcaster Count: 1			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/cf-broadcaster	1.13.0	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/cf-platform-analytics Count: 2			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/cf-platform-analytics	0.49.86	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/cf-platform-analytics	0.49.86	CVE-2024-27088	Our approach mitigates the vulnerability by enforcing simplified function naming conventions and prioritizing updated dependencies that prevent script stalls caused by complex function declarations

[CVE Mitigations from V2.2.5 to V2.6.9]

Image	Tag	CVE	Mitigation
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/cf-ui Count: 4			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/cf-ui	14.97.51	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/cf-ui	14.97.51	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/cf-ui	14.97.51	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/cf-ui	14.97.51	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/charts-manager Count: 1			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/charts-manager	1.22.3	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/context-manager Count: 6			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/context-manager	2.33.7	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/context-manager	2.33.7	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/context-manager	2.33.7	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/context-manager	2.33.7	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/context-manager	2.33.7	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/context-manager	2.33.7	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/gitops-dashboard-manager			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/gitops-dashboard-manager	1.14.22	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/runtime-environment-manager Count: 5			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/runtime-environment-manager	3.39.4	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.

CVE Mitigations from V2.2.5 to V2.6.9			

Image	Tag	CVE	Mitigation
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/runtime-environment-manager	3.39.4	CVE-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/runtime-environment-manager	3.39.4	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/runtime-environment-manager	3.39.4	CVE-2023-42363	The vulnerability affecting BusyBox and the xasprintf function does not affect the security of environments that use Node.js without using BusyBox directly
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/runtime-environment-manager	3.39.4	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/tasker-kubernetes Count: 1			
us-docker.pkg.dev/codefresh-enterprise/gcr.io/codefresh/tasker-kubernetes	1.26.18	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.