Codefresh On-premises CVE Mitigations

On-premises v2.4.2 CVE Mitigations

Version 2.4.2 Image	CVE ID	Image Version	Mitigation
codefresh/cf-api *Published on:* *July 5 2024*	**CVE-2021-3377**	21.253.43	The attacker cannot inject an XSS vulnerability into the logs due to our input validation. The only possible avenue for such an attack is to invoke an external service through a Codefresh step in the pipeline, which could potentially introduce HTML content into the logs. However, even in this scenario, Codefresh utilizes this library exclusively when a customer attempts to download logs in HTML format. This is distinct from the Codefresh logs viewer and is unrelated to it.
codefresh/cf-api *Published on:* *July 5 2024*	**CVE-2020-36604**	21.253.43	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/cf-api *Published on:* *July 5 2024*	**CVE-2023-42364**	21.253.43	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.
codefresh/cf-api *Published on:* *July 5 2024*	**CVE-2023-42365**	21.253.43	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.
codefresh/cf-broadcaster *Published on:* *July 5 2024*	**CVE-2023-42363**	1.12.14	The vulnerability affecting the *xasprintf* function in BusyBox does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.

Version 2.4.2			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/cf-broadcaster *Published on:* *July 5 2024*	**CVE-2020-36604**	1.12.14	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/cf-broadcaster *Published on:* *July 5 2024*	**CVE-2023-42365**	1.12.14	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.
codefresh/cf-broadcaster *Published on:* *July 5 2024*	**CVE-2023-42366**	1.12.14	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.
codefresh/cf-broadcaster *Published on:* *July 5 2024*	**CVE-2023-42364**	1.12.14	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.
codefresh/cf-platform-analytics *Published on:* *July 5 2024*	**CVE-2020-36604**	0.49.48	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/cf-platform-analytics *Published on:* *July 5 2024*	**CVE-2023-42363**	0.49.48	The vulnerability affecting the *xasprintf* function in BusyBox does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.

Version 2.4.2			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/cf-platform-analytics *Published on:* *July 5 2024*	**CVE-2023-42364**	0.49.48	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.
codefresh/cf-platform-analytics *Published on:* *July 5 2024*	**CVE-2023-42365**	0.49.48	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.
codefresh/cf-platform-analytics *Published on:* *July 5 2024*	**CVE-2024-27088**	0.49.48	Our approach mitigates the vulnerability by enforcing simplified function naming conventions and prioritizing updated dependencies to prevent script stalls caused by complex function declarations.
codefresh/cf-platform-analytics *Published on:* *July 5 2024*	**CVE-2023-50709**	0.49.48	Codefresh does not directly expose Cube API to the internet. We use a separate express.js server that uses the logic from cube.js to process the requests.
codefresh/cf-ui *Published on:* *July 5 2024*	**CVE-2023-42365**	14.94.77	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.
codefresh/cf-ui *Published on:* *July 5 2024*	**CVE-2023-42364**	14.94.77	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

Version 2.4.2			
Image	**CVE ID**	**Image Version**	**Mitigation**
			handling of file operations within our Node.js environment.
codefresh/charts-manager *Published on:* *July 5 2024*	**CVE-2020-36604**	1.17.2	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/charts-manager *Published on:* *July 5 2024*	**CVE-2023-42365**	1.17.2	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.
codefresh/charts-manager *Published on:* *July 5 2024*	**CVE-2023-42364**	1.17.2	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.
codefresh/cluster-providers *Published on:* *July 5 2024*	**CVE-2023-42364**	1.17.7	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.
codefresh/cluster-providers *Published on:* *July 5 2024*	**CVE-2023-42365**	1.17.7	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.

Version 2.4.2			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/cluster-providers *Published on:* *July 5 2024*	**CVE-2023-42363**	1.17.7	The vulnerability affecting the *xasprintf* function in BusyBox does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
codefresh/cluster-providers *Published on:* *July 5 2024*	**CVE-2023-42366**	1.17.7	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.
codefresh/consul *Published on:* *July 5 2024*	**PRISMA-2023-0056**	1.19.0-debian-12-r2	Latest upstream version.
codefresh/context-manager *Published on:* *July 5 2024*	**CVE-2020-36604**	2.29.4	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/context-manager *Published on:* *July 5 2024*	**CVE-2023-42364**	2.29.4	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.
codefresh/context-manager *Published on:* *July 5 2024*	**CVE-2023-42365**	2.29.4	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.

Version 2.4.2			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/docker *Published on:* *July 5 2024*	**CVE-2023-42363**	27.0-dind	Latest upstream version.
codefresh/docker *Published on:* *July 5 2024*	**CVE-2023-42365**	27.0-dind	Latest upstream version.
codefresh/docker *Published on:* *July 5 2024*	**CVE-2023-42366**	27.0-dind	Latest upstream version.
codefresh/gitops-dashboard-manager *Published on:* *July 5 2024*	**CVE-2020-36604**	1.14.13	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/gitops-dashboard-manager *Published on:* *July 5 2024*	**CVE-2023-42366**	1.14.13	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.
codefresh/gitops-dashboard-manager *Published on:* *July 5 2024*	**CVE-2023-42365**	1.14.13	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.
codefresh/gitops-dashboard-manager *Published on:* *July 5 2024*	**CVE-2023-42364**	1.14.13	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

Version 2.4.2			
Image	**CVE ID**	**Image Version**	**Mitigation**
			handling of file operations within our Node.js environment.
codefresh/gitops-dashboard-manager *Published on:* *July 5 2024*	**CVE-2023-42363**	1.14.13	The vulnerability affecting the *xasprintf* function in BusyBox does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
codefresh/kube-integration *Published on:* *July 5 2024*	**CVE-2023-42366**	1.31.8	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.
codefresh/kube-integration *Published on:* *July 5 2024*	**CVE-2023-42365**	1.31.8	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.
codefresh/kube-integration *Published on:* *July 5 2024*	**CVE-2023-42364**	1.31.8	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.
codefresh/kube-integration *Published on:* *July 5 2024*	**CVE-2023-42363**	1.31.8	The vulnerability affecting the *xasprintf* function in BusyBox does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.

Version 2.4.2			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/nginx-unprivileged *Published on:* *July 5 2024*	**CVE-2023-42366**	1.25-alpine	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.
codefresh/nginx-unprivileged *Published on:* *July 5 2024*	**CVE-2023-42365**	1.25-alpine	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.
codefresh/nginx-unprivileged *Published on:* *July 5 2024*	**CVE-2023-42364**	1.25-alpine	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.
codefresh/nginx-unprivileged *Published on:* *July 5 2024*	**CVE-2023-42363**	1.25-alpine	The vulnerability affecting the *xasprintf* function in BusyBox does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
codefresh/pipeline-manager *Published on:* *July 5 2024*	**CVE-2020-36604**	3.134.9	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.

Version 2.4.2			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/pipeline-manager *Published on:* *July 5 2024*	**CVE-2023-42364**	3.134.9	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.
codefresh/pipeline-manager *Published on:* *July 5 2024*	**CVE-2023-42365**	3.134.9	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.
codefresh/runtime-environment-manager *Published on:* *July 5 2024*	**CVE-2020-36604**	3.35.7	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/runtime-environment-manager *Published on:* *July 5 2024*	**CVE-2023-42364**	3.35.7	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.
codefresh/runtime-environment-manager *Published on:* *July 5 2024*	**CVE-2023-42365**	3.35.7	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.

Version 2.4.2			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/tasker-kubernetes *Published on:* *July 5 2024*	**CVE-2020-36604**	1.26.9	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/tasker-kubernetes *Published on:* *July 5 2024*	**CVE-2023-42363**	1.26.9	The vulnerability affecting the *xasprintf* function in BusyBox does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
codefresh/tasker-kubernetes *Published on:* *July 5 2024*	**CVE-2023-42364**	1.26.9	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.
codefresh/tasker-kubernetes *Published on:* *July 5 2024*	**CVE-2023-42365**	1.26.9	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.
codefresh/tasker-kubernetes *Published on:* *July 5 2024*	**CVE-2023-42366**	1.26.9	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.

On-premises v2.3.3 CVE Mitigations

Version 2.3.3 Image	CVE ID	Image Version	Mitigation
codefresh/cf-api *Published on:* *May 28 2024*	**CVE-2021-3377**	21.247.17	The attacker cannot inject an XSS vulnerability into the logs due to our input validation. The only possible avenue for such an attack is to invoke an external service through a Codefresh step in the pipeline, which could potentially introduce HTML content into the logs. However, even in this scenario, Codefresh utilizes this library exclusively when a customer attempts to download logs in HTML format. This is distinct from the Codefresh logs viewer and is unrelated to it.
codefresh/cf-api *Published on:* *May 28 2024*	**CVE-2020-36604**	21.247.15	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/cf-broadcaster *Published on:* *May 28 2024*	**CVE-2024-29041**	1.12.10	Related to improperly formed URL redirects in the Express.js framework which does not affect our service. Since our service does not utilize any redirect mechanisms, the risk posed by this vulnerability is not applicable to our application, and therefore no measures are necessary.
codefresh/cf-broadcaster *Published on:* *May 28 2024*	**CVE-2020-36604**	1.12.10	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/consul *Published on:* *May 28 2024*	**PRISMA-2023-0056**	1.18.0-debian-12-r0	Latest upstream version.
codefresh/cf-platform-analytics *Published on:* *May 28 2024*	**CVE-2020-36604**	0.49.37	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.

Version 2.3.3			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/cf-platform-analytics *Published on:* *May 28 2024*	**CVE-2023-50709**	0.49.37	Codefresh does not directly expose Cube API to the internet. We use a separate express.js server that uses the logic from cube.js to process the requests.
codefresh/cf-tls-sign *Published on:* *May 28 2024*	**CVE-2023-42282**	1.8.0	The 'ip' package is nested within the global NPM (Node Package Manager) repository. However, it remains unused for installing dependencies as we rely on yarn. Furthermore, it does not play a role in the service's runtime operations.
codefresh/cf-tls-sign *Published on:* *May 28 2024*	**CVE-2024-28863**	1.8.0	The tar package is on the third tier of dependencies in the cubejs-backend/api-gateway package. By not relying on user custom data input, the above mentioned NPM repository ensures that this specific vulnerability poses no threat to its functionality.
codefresh/charts-manager *Published on:* *May 28 2024*	**CVE-2020-36604**	1.16.12	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/context-manager *Published on:* *May 28 2024*	**CVE-2020-36604**	2.26.13	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/docker *Published on:* *May 28 2024*	**CVE-2023-45288**	26.0-dind	Latest upstream version.
codefresh/gitops-dashboard-manager *Published on:* *May 28 2024*	**CVE-2020-36604**	1.14.11	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/pipeline-manager	**CVE-2020-36604**	3.132.4	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate

Version 2.3.3 Image	CVE ID	Image Version	Mitigation
Published on: *May 28 2024*			threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/runtime-environment-manager *Published on:* *May 28 2024*	**CVE-2020-36604**	3.33.4	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/tasker-kubernetes *Published on:* *May 28 2024*	**CVE-2020-36604**	1.26.3	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/tasker-kubernetes *Published on:* *May 28 2024*	**CVE-2024-29041**	1.26.3	Related to improperly formed URL redirects in the Express.js framework which does not affect our service. Since our service does not utilize any redirect mechanisms, the risk posed by this vulnerability is not applicable to our application, and therefore no measures are necessary.

On-premises v2.3 CVE Mitigations

Version 2.3 Image	CVE ID	Image Version	Mitigation
codefresh/argo-platform-abac *Published on:* *March 28 2024*	**CVE-2023-26108**	1.2577.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-api-events *Published on:* *March 28 2024*	**CVE-2023-26108**	1.2577.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-api-graphql *Published on:* *March 28 2024*	**CVE-2023-26108**	1.2577.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-audit *Published on:* *March 28 2024*	**CVE-2023-26108**	1.2577.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-analytics-reporter *Published on:* *March 28 2024*	**CVE-2023-26108**	1.2577.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-cron-executor *Published on:* *March 28 2024*	**CVE-2023-26108**	1.2577.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-event-handler *Published on:* *March 28 2024*	**CVE-2023-26108**	1.2577.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.

Version 2.3			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/cf-broadcaster *Published on:* *March 28 2024*	**CVE-2020-36604**	1.12.8	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/cf-api *Published on:* *March 28 2024*	**CVE-2021-3377**	21.47.15	The attacker cannot inject an XSS vulnerability into the logs due to our input validation. The only possible avenue for such an attack is to invoke an external service through a Codefresh step in the pipeline, which could potentially introduce HTML content into the logs. However, even in this scenario, Codefresh utilizes this library exclusively when a customer attempts to download logs in HTML format. This is distinct from the Codefresh logs viewer and is unrelated to it.
codefresh/cf-api *Published on:* *March 28 2024*	**CVE-2020-36604**	21.247.15	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/cf-platform-analytics *Published on:* *March 28 2024*	**CVE-2022-33987**	0.49.23	A deprecated version of got was built into Node.js, which (got) is not used in the platform at all.
codefresh/cf-platform-analytics *Published on:* *March 28 2024*			The dependency is present in the NPM (Node Package Manager) repository, but is not actually related to or used in the application's package or runtime.
codefresh/cf-platform-analytics *Published on:* *March 28 2024*	**CVE-2022-25881**	0.49.23	The dependency is present in the NPM (Node Package Manager) repository, but is not actually related to or used in the application's package or runtime.
codefresh/cf-platform-analytics *Published on:* *March 28 2024*	**CVE-2020-36604**	0.49.23	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.

Version 2.3 Image	CVE ID	Image Version	Mitigation
codefresh/cf-platform-analytics *Published on:* *March 28 2024*	**CVE-2023-50709**	0.49.23	Codefresh does not directly expose Cube API to the internet. We use a separate express.js server that uses the logic from cube.js to process the requests.
codefresh/cf-platform-analytics *Published on:* *March 28 2024*	**CVE-2022-25883**	0.49.23	Node.js includes a deprecated version of SemVer. Codefresh uses an updated SemVer version.
codefresh/cf-platform-analytics *Published on:* *March 28 2024*	**CVE-2024-0727**	0.49.23	The project utilizes OpenSSL embedded within Node.js, and the presence of OpenSSL within the APK package does not impact its functionality.
codefresh/cf-platform-analytics *Published on:* *March 28 2024*	**CVE-2021-3807**	0.49.23	The dependency is present in the NPM (Node Package Manager) repository, but is not actually related to or used in the application's package or runtime.
codefresh/charts-manager *Published on:* *March 28 2024*	**CVE-2020-36604**	1.16.9	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/cluster-providers *Published on:* *March 28 2024*	**CVE-2023-48795**	1.17.1	The latest image scans by both Prisma Cloud and Docker Scout did not detect any vulnerabilities.
codefresh/consul *Published on:* *March 28 2024*	**CVE-2023-0056**	1.17.0-debian-11-r1	Latest upstream version.
codefresh/context-manager *Published on:* *June 26 2024*	**CVE-2020-36604**	2.26.13	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.

Version 2.3			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/docker *Published on:* *April 16 2024*	**CVE-2023-47108**	25.0-dind	Docker daemon has a hidden /grpc endpoint not described in the documentation, containing an OpenTelemetry interceptor that gathers some metrics on it. Potentially excess usage of this endpoint can overflow the interceptor with metrics and bring the server down. However, for this you need to know which grpc method to use, which is not described in any public documentation. Furthermore, to access docker daemon via TCP in our setup, you require access to the SSL certificate stored in the secret. Only cf-builder and engine in Codefresh setup has access to this secret.
codefresh/gitops-dashboard-manager *Published on:* *March 28 2024*	**CVE-2020-36604**	1.14.8	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/gitops-dashboard-manager *Published on:* *March 28 2024*	**CVE-2023-48795**	1.14.8	The latest image scans by both Prisma Cloud and Docker Scout did not detect any vulnerabilities.
codefresh/kube-integration *Published on:* *March 28 2024*	**CVE-2023-48795**	1.31.3	The latest image scans by both Prisma Cloud and Docker Scout did not detect any vulnerabilities.
codefresh/pipeline-manager *Published on:* *March 28 2024*	**CVE-2020-36604**	3.132.3	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/runtime-environment-manager *Published on:* *March 28 2024*	**CVE-2020-36604**	3.33.2	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.

Version 2.3			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/tasker-kubernetes *Published on:* *March 24 2024*	**CVE-2020-36604**	1.25.2	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.

On-premises v2.2.5 CVE Mitigations

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/argo-hub-platform *Published on:* *Jan 31 2024*	**CVE-2022-2564**	0.1.8	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-abac *Published on:* *Jan 31 2024*	**CVE-2023-26108**	1.2527.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-abac *Last updated on* *Jan 31 2024*	**CVE-2023-3696**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-analytics-reporter *Published on:* *Jan 31 2024*	**CVE-2023-3696**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-analytics-reporter *Published on:* *Jan 31 2024*	**CVE-2023-26108**	1.2527.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-analytics-reporter *Published on:* *Jan 31 2024*	**CVE-2022-2564**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/argo-platform-analytics-reporter *Published on:* *Jan 31 2024*	**CVE-2021-32050**	1.2527.0	This issue does affect our application as Command Listener is disabled by default, and we don't enable it.
codefresh/argo-platform-api-events *Published on:* *Jan 31 2024*	**CVE-2023-3696**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-api-events *Published on:* *Jan 31 2024*	**CVE-2021-32050**	1.2527.0	This issue does affect our application as Command Listener is disabled by default, and we don't enable it.
codefresh/argo-platform-api-events *Published on:* *Jan 31 2024*	**CVE-2023-26108**	1.2527.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-api-events *Published on:* *Jan 31 2024*	**CVE-2022-2564**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-api-events *Published on:* *Jan 31 2024*	**CVE-2023-26108**	1.2527.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-api-graphql *Published on:* *Jan 31 2024*	**CVE-2023-26108**	1.2527.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/argo-platform-api-graphql *Published on:* *Jan 31 2024*	**CVE-2023-3696**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-api-graphql *Published on:* *Jan 31 2024*	**CVE-2021-32050**	1.2527.0	This issue does affect our application as Command Listener is disabled by default, and we don't enable it.
codefresh/argo-platform-api-graphql *Published on:* *Jan 31 2024*	**CVE-2023-26108**	1.2527.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-api-graphql *Published on:* *Jan 31 2024*	**CVE-2022-2564**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-audit *Published on:* *Jan 31 2024*	**CVE-2023-26108**	1.2527.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-audit *Published on:* *Jan 31 2024*	**CVE-2023-3696**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-audit *Published on:* *Jan 31 2024*	**CVE-2021-32050**	1.2527.0	This issue does affect our application as Command Listener is disabled by default, and we don't enable it.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/argo-platform-audit *Published on:* *Jan 31 2024*	**CVE-2022-2564**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-cron-executor *Published on:* *Jan 31 2024*	**CVE-2022-2564**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-cron-executor *Published on:* *Jan 31 2024*	**CVE-2021-32050**	1.2527.0	This issue does affect our application as Command Listener is disabled by default, and we don't enable it.
codefresh/argo-platform-cron-executor *Published on:* *Jan 31 2024*	**CVE-2023-26108**	1.2527.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-event-handler *Published on:* *Jan 31 2024*	**CVE-2023-26108**	1.2527.0	The identified vulnerability is associated with the StreamableFile API. Codefresh does not utilize the StreamableFile API for returning files. Additionally, we do not allow downloading of files from our services.
codefresh/argo-platform-event-handler *Published on:* *Jan 31 2024*	**CVE-2021-32050**	1.2527.0	This issue does affect our application as Command Listener is disabled by default, and we don't enable it.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/argo-platform-event-handler *Published on:* *Jan 31 2024*	**CVE-2022-2564**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/argo-platform-event-handler *Published on:* *Jan 31 2024*	**CVE-2023-3696**	1.2527.0	The application is safeguarded against Prototype Pollution in Mongoose, as it enforces request payload validation and does not pass any additional, potentially harmful data into Mongoose methods. This security measure prevents attackers from injecting malicious changes to the application's object prototypes.
codefresh/cf-api *Published on:* *Jan 31 2024*	**CVE-2021-3377**	21.234.11	The attacker cannot inject an XSS vulnerability into the logs due to our input validation. The only possible avenue for such an attack is to invoke an external service through a Codefresh step in the pipeline, which could potentially introduce HTML content into the logs. However, even in this scenario, Codefresh utilizes this library exclusively when a customer attempts to download logs in HTML format. This is distinct from the Codefresh logs viewer and is unrelated to it.
codefresh/cf-api *Published on:* *Jan 31 2024*	**CVE-2020-36604**	21.234.11	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/cf-platform-analytics *Published on:* *Jan 31 2024*	**CVE-2020-36604**	0.49.20	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/cf-platform-analytics *Published on:* *Jan 31 2024*	**CVE-2023-50709**	0.49.20	Codefresh does not directly expose Cube API to the internet. We use a separate express.js server that uses the logic from cube.js to process the requests.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/cf-platform-analytics *Published on: Jan 31 2024*	**CVE-2023-26136**	0.49.20	The dependency is present in the NPM (Node Package Manager) repository, but is not actually related to or used in the application's package or runtime.
codefresh/cf-platform-analytics *Published on: Jan 31 2024*	**CVE-2022-25881**	0.49.20	The dependency is present in the NPM (Node Package Manager) repository, but is not actually related to or used in the application's package or runtime.
codefresh/cf-platform-analytics *Published on: Jan 31 2024*	**CVE-2021-3807**	0.49.20	The dependency is present in the NPM (Node Package Manager) repository, but is not actually related to or used in the application's package or runtime.
codefresh/cf-platform-analytics*Published on: Jan 31 2024*	**CVE-2022-33987**	0.49.20	The dependency is present in the NPM (Node Package Manager) repository, but is not actually related to or used in the application's package or runtime.
codefresh/cf-platform-analytics *Published on: Jan 31 2024*	**CVE-2022-25883**	0.49.20	The dependency is present in the NPM (Node Package Manager) repository, but is not actually related to or used in the application's package or runtime.
codefresh/charts-manager *Published on: Jan 31 2024*	**CVE-2020-36604**	1.16.7	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/cluster-providers *Published on: Jan 31 2024*	**CVE-2023-48795**	1.17.0	The OpenSSH package with the vulnerability is included in the Alpine image used as the base image. Our microservice does not utilize this OpenSSH package, and it does not function as an SSH server or client in any capacity.
codefresh/gitops-dashboard-manager*Published on: Jan 31 2024*	**CVE-2020-36604**	1.14.7	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
codefresh/gitops-dashboard-manager *Published on:* *Jan 31 2024*	**CVE-2023-48795**	1.14.7	The OpenSSH package with the vulnerability is included in the Alpine image used as the base image. Our microservice does not utilize this OpenSSH package, and it does not function as an SSH server or client in any capacity.
codefresh/hermes *Published on:* *Jan 31 2024*	**CVE-2023-39325**	0.21.7	Image is not used.
codefresh/kube-integration *Published on:* *Jan 31 2024*	**CVE-2023-48795**	1.31.2	The OpenSSH package with the vulnerability is included in the Alpine image used as the base image. Our microservice does not utilize this OpenSSH package, and it does not function as an SSH server or client in any capacity.
codefresh/pipeline-manager *Published on:* *Jan 31 2024*	**CVE-2020-36604**	3.131.15	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/runtime-environment-manager *Published on:* *Jan 31 2024*	**CVE-2023-43646**	3.33.2	The vulnerable functionality of this package is not used in the runtime-environment-manager.
codefresh/runtime-environment-manager *Published on:* *Jan 31 2024*	**CVE-2022-25883**	3.33.2	The dependency is present in the NPM (Node Package Manager) repository, but is not actually related to or used in the application's package or runtime.
codefresh/tasker-kubernetes *Published on:* *Jan 31 2024*	**CVE-2020-36604**	1.25.0	Risk assessment confirms Hoek vulnerability which is unused and does not pose an immediate threat. An update is scheduled for the next update cycle following a full review and thorough testing.
codefresh/tasker-kubernetes *Published on:* *Jan 31 2024*	**CVE-2023-48795**	1.25.0	The OpenSSH package with the vulnerability is included in the Alpine image used as the base image. Our microservice does not utilize this OpenSSH package, and it does not function as an SSH server or client in any capacity.