Codefresh On-premises CVE Mitigations

On-premises CVE Mitigations

Codefresh continuously addresses security concerns and implements vulnerability fixes for our On-premises versions.

This document focuses on and serves as a reference for Common Vulnerabilities and Exposures (CVEs) with mitigations.

The CVEs are categorized by each on-premises version, starting with V2.2.5. They are organized in tables by Image name, CVE ID, Image Version and Mitigation. The tables are sorted by the Image names.

The document is updated per on-premises version to ensure that you stay informed about the specific CVE mitigations relevant to your Codefresh on-premises installation. Every Image includes the Published On date identifying the date of the most recent update.

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.

Version 2.3			
Image	**CVE ID**	**Image Version**	**Mitigation**
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.
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*	**CVE-2023-26136**	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.

Version 2.3			
Image	**CVE ID**	**Image Version**	**Mitigation**
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.
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.

Version 2.3			
Image	**CVE ID**	**Image Version**	**Mitigation**
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:* *March 28 2024*	**CVE-2020-36604**	2.26.12	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/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

Version 2.3 Image	CVE ID	Image Version	Mitigation
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.
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.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
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
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.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
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.
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.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
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.
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.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
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.
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.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
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.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
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.
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.

Version 2.2.5			
Image	**CVE ID**	**Image Version**	**Mitigation**
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.