

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 version includes the Last Updated On date displayed in the footer identifies the date of the most recent update.

On-premises v2.2.5: CVE Mitigations

Image	CVE ID	Image Version	Mitigation
codefresh/argo-hub-platform <i>Published on: Jan 31 2024</i>	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 <i>Published on: Jan 31 2024</i>	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 <i>Last updated on Jan 31 2024</i>	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 <i>Published on: Jan 31 2024</i>	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 <i>Published on: Jan 31 2024</i>	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.

Image	CVE ID	Image Version	Mitigation
codefresh/argo-platform-analytics-reporter <i>Published on: Jan 31 2024</i>	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 <i>Published on: Jan 31 2024</i>	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 <i>Published on: Jan 31 2024</i>	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 <i>Published on: Jan 31 2024</i>	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 <i>Published on: Jan 31 2024</i>	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 <i>Published on: Jan 31 2024</i>	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.

Image	CVE ID	Image Version	Mitigation
codefresh/argo-platfor m-api-events <i>Published on: Jan 31 2024</i>	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-platfor m-api-graphql <i>Published on: Jan 31 2024</i>	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-platfor m-api-graphql <i>Published on: Jan 31 2024</i>	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-platfor m-api-graphql <i>Published on: Jan 31 2024</i>	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-platfor m-api-graphql <i>Published on: Jan 31 2024</i>	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-platfor m-api-graphql <i>Published on: Jan 31 2024</i>	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.

Image	CVE ID	Image Version	Mitigation
codefresh/argo-platfor m-audit <i>Published on: Jan 31 2024</i>	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-platfor m-audit <i>Published on: Jan 31 2024</i>	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-platfor m-audit <i>Published on: Jan 31 2024</i>	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-platfor m-audit <i>Published on: Jan 31 2024</i>	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-platfor m-cron-executor <i>Published on: Jan 31 2024</i>	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-platfor m-cron-executor <i>Published on: Jan 31 2024</i>	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.

Image	CVE ID	Image Version	Mitigation
codefresh/argo-platfor m-cron-executor <i>Published on: Jan 31 2024</i>	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-platfor m-event-handler <i>Published on: Jan 31 2024</i>	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-platfor m-event-handler <i>Published on: Jan 31 2024</i>	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-platfor m-event-handler <i>Published on: Jan 31 2024</i>	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-platfor m-event-handler <i>Published on: Jan 31 2024</i>	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.

Image	CVE ID	Image Version	Mitigation
codefresh/cf-api <i>Published on:</i> <i>Jan 31 2024</i>	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 <i>Published on:</i> <i>Jan 31 2024</i>	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 <i>Published on:</i> <i>Jan 31 2024</i>	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 <i>Published on:</i> <i>Jan 31 2024</i>	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.
codefresh/cf-platform -analytics <i>Published on:</i> <i>Jan 31 2024</i>	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 <i>Published on:</i> <i>Jan 31 2024</i>	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.

Image	CVE ID	Image Version	Mitigation
codefresh/cf-platform -analytics <i>Published on:</i> <i>Jan 31 2024</i>	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 <i>Published on:</i> <i>Jan 31 2024</i>	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 <i>Published on:</i> <i>Jan 31 2024</i>	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-man ager <i>Published on:</i> <i>Jan 31 2024</i>	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-pro viders <i>Published on:</i> <i>Jan 31 2024</i>	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-dash board-manager <i>Published on:</i> <i>Jan 31 2024</i>	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-dash board-manager <i>Published on:</i> <i>Jan 31 2024</i>	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.

Image	CVE ID	Image Version	Mitigation
codefresh/hermes <i>Published on:</i> <i>Jan 31 2024</i>	CVE-2023-39325	0.21.7	Image is not used.
codefresh/kube-integration <i>Published on:</i> <i>Jan 31 2024</i>	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 <i>Published on:</i> <i>Jan 31 2024</i>	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 <i>Published on:</i> <i>Jan 31 2024</i>	CVE-2023-43646	3.33.2	The vulnerable functionality of this package is not used in the runtime-environment-manager.
codefresh/runtime-environment-manager <i>Published on:</i> <i>Jan 31 2024</i>	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 <i>Published on:</i> <i>Jan 31 2024</i>	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 <i>Published on:</i> <i>Jan 31 2024</i>	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.