

Gitops-runtime Version 0.26.4 - Published 22 December 2025			
Image	Tag	CVE	Mitigation
argocd	v3.2.2	CVE-2025-64329	The vulnerability in containerd's CRI Attach implementation, causing a memory exhaustion issue due to goroutine leaks in containerd (the container runtime), not ArgoCD. ArgoCD has not even a library dependency on this specific software.

Gitops-runtime Version 0.25.1 - Published 6 November 2025			
Image	Tag	CVE	Mitigation
cf-argocd-extras	5a607d5	CVE-2025-0426	Argo service does not directly interact with kubelet endpoints. It communicates exclusively with the Kubernetes API server (kube-apiserver) to manage the desired state of applications. Therefore, the service does not make any requests to kubelet's read-only or write endpoints, nor does it depend on this functionality for its operation. As a result, this vulnerability does not directly impact the functionality.
cf-argocd-extras	5a607d5	CVE-2024-9042	This vulnerability is not applicable to Argo services, as it cannot be deployed on Windows nodes. The service runs exclusively on Linux-based nodes, and the affected /logs/query API endpoint is only present and exploitable on Windows nodes. Therefore, this issue does not pose any risk to Argo environments.
argo-events	v1.9.2-cap-CR-30841	CVE-2025-30204	The argo-events component includes github.com/golang-jwt/jwt as a transitive dependency through the module github.com/Azure/azure-sdk-for-go/sdk/storage/azqueue . This library is not used directly by our service logic, and no JWT token parsing or validation is performed via this path. Therefore, any potential issues or vulnerabilities in github.com/golang-jwt/jwt do not affect the behavior or security of our service.
natsio/prometheus-nats-exporter	0.16.0	CVE-2025-26519	To avoid the vulnerability we it is needed to delete all overrides of "prometheus-nats-exporter" itself if it exists. And upgrade gitops-runtime with values \$ global: runtime: eventBus: type: jetstream
natsio/prometheus-nats-exporter	0.16.0	CVE-2025-30215	To avoid the vulnerability we it is needed to delete all overrides of "prometheus-nats-exporter" itself if it exists. And upgrade gitops-runtime with values \$ global: runtime: eventBus: type: jetstream
natsio/prometheus-nats-exporter	0.16.0	CVE-2024-12797	To avoid the vulnerability we it is needed to delete all overrides of "prometheus-nats-exporter" itself if it exists. And upgrade gitops-runtime with values \$ global: runtime: eventBus: type: jetstream
natsio/prometheus-nats-exporter	0.16.0	CVE-2024-13176	To avoid the vulnerability we it is needed to delete all overrides of "prometheus-nats-exporter" itself if it exists. And upgrade gitops-runtime with values \$ global: runtime: eventBus: type: jetstream

Gitops-runtime Version 0.23.1 - Published 21 August 2025				
Image	Tag	CVE	Mitigation	
cf-argocd-extras	v0.5.12	CVE-2025-0426	<p>Summary: CVE-2025-0426 describes a Denial of Service vulnerability in the Kubernetes kubelet component, where unauthenticated requests to the read-only HTTP endpoint can fill up node disk space via the checkpoint API, potentially leading to node unavailability.</p> <p>Mitigation: Argo service does not directly interact with kubelet endpoints. It communicates exclusively with the Kubernetes API server (kube-apiserver) to manage the desired state of applications. Therefore, the service does not make any requests to kubelet's read-only or write endpoints, nor does it depend on this functionality for its operation. As a result, this vulnerability does not directly impact the functionality.</p>	
cf-argocd-extras	v0.5.12	CVE-2024-9042	This vulnerability is not applicable to Argo services, as it cannot be deployed on Windows nodes. The service runs exclusively on Linux-based nodes, and the affected /logs/query API endpoint is only present and exploitable on Windows nodes. Therefore, this issue does not pose any risk to Argo environments.	
redis	7.4.5-alpine	CVE-2022-30632	CVE-2022-30632 vulnerability in Go's path/filepath.Glob library, affecting gosu (if compiled with an old Go version), does not impact Redis's functionality or security. Redis is written in C and doesn't use Go's path/filepath.Glob. While gosu is a Go binary often found in Redis Docker images, its role is to safely switch user privileges, not to process arbitrary paths in a way that would trigger this specific stack exhaustion vulnerability. Therefore, there's no direct threat to Redis itself from this particular Go vulnerability.	
redis	7.4.5-alpine	CVE-2022-30630	CVE-2022-30630 do not impact Redis because Redis itself is written in C, not Go, and therefore does not use Go's io/fs or path/filepath libraries. The gosu utility, although a Go binary often present in Redis images, is used for user switching, not for processing file paths in a way that would trigger these specific Glob vulnerabilities. Thus, the core Redis functionality and its data remain unaffected.	
redis	7.4.5-alpine	CVE-2023-29403	CVE-2023-29403 (GO-2023-1840), does not directly impact Redis's operation. This is because Redis itself is written in C, not Go, and therefore doesn't use the Go runtime or its libraries where the vulnerability lies. While the gosu utility, often found in Redis Docker images, is a Go binary, its function doesn't involve scenarios that would exploit this specific vulnerability. In essence, gosu isn't designed to perform the kind of file operations or register handling that would trigger the issues described in this CVE.	
argocli	v3.6.7-cap-CR-28355	CVE-2025-8556	The vulnerable code is not reachable or executable from any argocli code path. The code does not use CIRCL's FourQ implementation. Also it does not invoke vulnerable cryptographic functions.	

Gitops-runtime Version 0.22.2 - Published 04 August 2025			
Image	Tag	CVE	Mitigation
cf-argocd-extras	0.5.7	CVE-2025-0426	<p>Summary: CVE-2025-0426 describes a Denial of Service vulnerability in the Kubernetes kubelet component, where unauthenticated requests to the read-only HTTP endpoint can fill up node disk space via the checkpoint API, potentially leading to node unavailability.</p> <p>Mitigation: Argo service does not directly interact with kubelet endpoints. It communicates exclusively with the Kubernetes API server (kube-apiserver) to manage the desired state of applications. Therefore, the service does not make any requests to kubelet's read-only or write endpoints, nor does it depend on this functionality for its operation. As a result, this vulnerability does not directly impact the functionality.</p>
cf-argocd-extras	0.5.7	CVE-2024-9042	This vulnerability is not applicable to Argo services, as it cannot be deployed on Windows nodes. The service runs exclusively on Linux-based nodes, and the affected /logs/query API endpoint is only present and exploitable on Windows nodes. Therefore, this issue does not pose any risk to Argo environments.
redis	7.4.2-alpine	CVE-2022-30632	CVE-2022-30632 vulnerability in Go's path/filepath.Glob library, affecting gosu (if compiled with an old Go version), does not impact Redis's functionality or security. Redis is written in C and doesn't use Go's path/filepath.Glob. While gosu is a Go binary often found in Redis Docker images, its role is to safely switch user privileges, not to process arbitrary paths in a way that would trigger this specific stack exhaustion vulnerability. Therefore, there's no direct threat to Redis itself from this particular Go vulnerability.
redis	7.4.2-alpine	CVE-2022-30630	CVE-2022-30630 do not impact Redis because Redis itself is written in C, not Go, and therefore does not use Go's io/fs or path/filepath libraries. The gosu utility, although a Go binary often present in Redis images, is used for user switching, not for processing file paths in a way that would trigger these specific Glob vulnerabilities. Thus, the core Redis functionality and its data remain unaffected.
redis	7.4.2-alpine	CVE-2023-29403	CVE-2023-29403 (GO-2023-1840), does not directly impact Redis's operation. This is because Redis itself is written in C, not Go, and therefore doesn't use the Go runtime or its libraries where the vulnerability lies. While the gosu utility, often found in Redis Docker images, is a Go binary, its function doesn't involve scenarios that would exploit this specific vulnerability. In essence, gosu isn't designed to perform the kind of file operations or register handling that would trigger the issues described in this CVE.

Onprem Version 2.8.10 - Published 28 July 2025			
Image	Tag	CVE	Mitigation
argo-platform-abac	1.3525.2-onprem-45cda44	CVE-2023-26108	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.
argo-platform-abac	1.3525.2-onprem-45cda44	CVE-2024-29409	CVE-2024-29409 describes a file upload vulnerability in NestJS Nest v10.3.2. This flaw allows a remote attacker to achieve remote code execution by manipulating the Content-Type header during a file upload, tricking the application into processing a malicious file. Our services are not impacted by this vulnerability because our applications do not use file upload functionalities. The vulnerability is specifically tied to the file upload mechanism in NestJS; since our systems do not have this feature enabled, there is no risk of a malicious file being uploaded or executed.
argo-platform-analytics-reporter	1.3525.2-onprem-45cda44	CVE-2023-26108	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.
argo-platform-analytics-reporter	1.3525.2-onprem-45cda44	CVE-2024-29409	CVE-2024-29409 describes a file upload vulnerability in NestJS Nest v10.3.2. This flaw allows a remote attacker to achieve remote code execution by manipulating the Content-Type header during a file upload, tricking the application into processing a malicious file. Our services are not impacted by this vulnerability because our applications do not use file upload functionalities. The vulnerability is specifically tied to the file upload mechanism in NestJS; since our systems do not have this feature enabled, there is no risk of a malicious file being uploaded or executed.
argo-platform-api-events	1.3525.2-onprem-45cda44	CVE-2023-26108	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.
argo-platform-api-events	1.3525.2-onprem-45cda44	CVE-2024-29409	CVE-2024-29409 describes a file upload vulnerability in NestJS Nest v10.3.2. This flaw allows a remote attacker to achieve remote code execution by manipulating the Content-Type header during a file upload, tricking the application into processing a malicious file. Our services are not impacted by this vulnerability because our applications do not use file upload functionalities. The vulnerability is specifically tied to the file upload mechanism in NestJS; since our systems do not have this feature enabled, there is no risk of a malicious file being uploaded or executed.
argo-platform-api-graphql	1.3525.2-onprem-45cda44	CVE-2023-26108	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.
argo-platform-api-graphql	1.3525.2-onprem-45cda44	CVE-2024-29409	CVE-2024-29409 describes a file upload vulnerability in NestJS Nest v10.3.2. This flaw allows a remote attacker to achieve remote code execution by manipulating the Content-Type header during a file upload, tricking the application into processing a malicious file. Our services are not impacted by this vulnerability because our applications do not use file upload functionalities. The vulnerability is specifically tied to the file upload mechanism in NestJS; since our systems do not have this feature enabled, there is no risk of a malicious file being uploaded or executed.
argo-platform-api-graphql	1.3525.2-onprem-45cda44	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.
argo-platform-audit	1.3525.2-onprem-45cda44	CVE-2023-26108	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.
argo-platform-audit	1.3525.2-onprem-45cda44	CVE-2024-29409	CVE-2024-29409 describes a file upload vulnerability in NestJS Nest v10.3.2. This flaw allows a remote attacker to achieve remote code execution by manipulating the Content-Type header during a file upload, tricking the application into processing a malicious file. Our services are not impacted by this vulnerability because our applications do not use file upload functionalities. The vulnerability is specifically tied to the file upload mechanism in NestJS; since our systems do not have this feature enabled, there is no risk of a malicious file being uploaded or executed.
argo-platform-broadcaster	1.3525.2-onprem-45cda44	CVE-2023-26108	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.
argo-platform-broadcaster	1.3525.2-onprem-45cda44	CVE-2024-29409	CVE-2024-29409 describes a file upload vulnerability in NestJS Nest v10.3.2. This flaw allows a remote attacker to achieve remote code execution by manipulating the Content-Type header during a file upload, tricking the application into processing a malicious file. Our services are not impacted by this vulnerability because our applications do not use file upload functionalities. The vulnerability is specifically tied to the file upload mechanism in NestJS; since our systems do not have this feature enabled, there is no risk of a malicious file being uploaded or executed.
argo-platform-cron-executor	1.3525.2-onprem-45cda44	CVE-2024-29409	CVE-2024-29409 describes a file upload vulnerability in NestJS Nest v10.3.2. This flaw allows a remote attacker to achieve remote code execution by manipulating the Content-Type header during a file upload, tricking the application into processing a malicious file. Our services are not impacted by this vulnerability because our applications do not use file upload functionalities. The vulnerability is specifically tied to the file upload mechanism in NestJS; since our systems do not have this feature enabled, there is no risk of a malicious file being uploaded or executed.
argo-platform-cron-executor	1.3525.2-onprem-45cda44	CVE-2023-26108	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.
argo-platform-event-handler	1.3525.2-onprem-45cda44	CVE-2024-29409	CVE-2024-29409 describes a file upload vulnerability in NestJS Nest v10.3.2. This flaw allows a remote attacker to achieve remote code execution by manipulating the Content-Type header during a file upload, tricking the application into processing a malicious file. Our services are not impacted by this vulnerability because our applications do not use file upload functionalities. The vulnerability is specifically tied to the file upload mechanism in NestJS; since our systems do not have this feature enabled, there is no risk of a malicious file being uploaded or executed.
argo-platform-event-handler	1.3525.2-onprem-45cda44	CVE-2023-26108	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.
argo-platform-promotion-orchestrator	1.3525.2-onprem-45cda44	CVE-2024-29409	CVE-2024-29409 describes a file upload vulnerability in NestJS Nest v10.3.2. This flaw allows a remote attacker to achieve remote code execution by manipulating the Content-Type header during a file upload, tricking the application into processing a malicious file. Our services are not impacted by this vulnerability because our applications do not use file upload functionalities. The vulnerability is specifically tied to the file upload mechanism in NestJS; since our systems do not have this feature enabled, there is no risk of a malicious file being uploaded or executed.
argo-platform-promotion-orchestrator	1.3525.2-onprem-45cda44	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.
argo-platform-promotion-orchestrator	1.3525.2-onprem-45cda44	CVE-2023-26108	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.
cf-api	21.279.7	CVE-2024-11023	CVE-2024-11023: Firebase JavaScript SDK utilizes a "FIREBASE_DEFAULTS" cookie to store configuration data, including an "_authTokenSyncURL" field used 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 an 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.

cf-api	21.279.7	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.
cf-api	21.279.7	CVE-2021-3377	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 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.
cf-api	21.279.7	CVE-2022-23539	We do not configure the jsonwebtoken library to use custom key types or algorithms, thus the default settings are used. As a result, the vulnerability does not affect our application since it only impacts configurations using invalid key types / algorithm combinations, which we do not utilize.
cf-broadcaster	1.13.2	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.
cf-container-logger	1.12.8	CVE-2024-11023	CVE-2024-11023: Firebase JavaScript SDK utilizes a "FIREBASE_DEFAULTS" cookie to store configuration data, including an "_authTokenSyncURL" field used 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 an actor to capture user session data transmitted by the SDK.
cf-deploy-kubernetes	16.2.9	CVE-2023-42364	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.
cf-deploy-kubernetes	16.2.9	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	16.2.9	CVE-2023-42363	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	16.2.9	CVE-2023-42366	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
cf-deploy-kubernetes	16.2.9	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	10.3.2	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-platform-analytics	0.50.4	CVE-2022-36313	The vulnerable package "file-type" is nested in "decompress" package.
cf-platform-analytics	0.50.4	CVE-2020-36604	The CVE-2022-36313 vulnerability relates specifically to .mkv file type handling. The decompress package utilizes file-type exclusively for detecting types such as tar, tarbz2, targz, and zip. Therefore, the service is not affected by this vulnerability.
charts-manager	1.23.3	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.
consul	1.21.2-debian-12-r0	PRISMA-2023-0056	Our approach mitigates the vulnerability by enforcing simplified function naming conventions and prioritizing updated dependencies that prevent script stalls caused by complex function declarations
context-manager	2.34.4	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.
engine	1.178.2	CVE-2024-11023	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	1.178.2	CVE-2020-36604	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	1.178.2	CVE-2024-29415	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	1.178.2	CVE-2024-28176	This package is not used inside our business logic to validate the loopback addresses thus we are not affected by this vulnerability.
gitops-dashboard-manager	1.14.24	CVE-2020-36604	Service utilizes the jose module as nested module in jsonwebtoken. 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
pipeline-manager	3.139.4	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.
runtime-environment-manager	3.41.3	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.
tasker-kubernetes	1.26.20	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.

Gitops-runtime Version 0.21.0 - Published 01 July 2025				
Image	Tag	CVE	Mitigation	
argocd	v2.14.9-2025-06-08-8821b48e	CVE-2025-0426	<p>Summary: CVE-2025-0426 describes a Denial of Service vulnerability in the Kubernetes kubelet component, where unauthenticated requests to the read-only HTTP endpoint can fill up node disk space via the checkpoint API, potentially leading to node unavailability.</p> <p>Mitigation: Argo service does not directly interact with kubelet endpoints. It communicates exclusively with the Kubernetes API server (kube-apiserver) to manage the desired state of applications. Therefore, the service does not make any requests to kubelet's read-only or write endpoints, nor does it depend on this functionality for its operation. As a result, this vulnerability does not directly impact the functionality.</p>	
argocd	v2.14.9-2025-06-08-8821b48e	CVE-2024-40635	<p>Summary: CVE-2024-40635 describes an integer overflow vulnerability in containerd where specifying a UID or GID greater than the maximum 32-bit signed integer (2147483647) can result in the container running as root (UID 0), even if configured to run as a non-root user.</p> <p>Mitigation: This vulnerability is only triggered during the image build stage, specifically while installing Helm in the Dockerfile. It does not affect ArgoCD at runtime, as the build-time environment is isolated from the container runtime used in Kubernetes.</p>	
argocd	v2.14.9-2025-06-08-8821b48e	CVE-2024-9042	This vulnerability is not applicable to Argo services, as it cannot be deployed on Windows nodes. The service runs exclusively on Linux-based nodes, and the affected /logs/query API endpoint is only present and exploitable on Windows nodes. Therefore, this issue does not pose any risk to Argo environments.	
prometheus-nats-exporter	0.15.0	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.	
prometheus-nats-exporter	0.15.0	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.	
prometheus-nats-exporter	0.15.0	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.	
prometheus-nats-exporter	0.15.0	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.	
argo-rollouts	v1.7.2-cap-CR-28008	CVE-2025-0426	<p>Summary: CVE-2025-0426 describes a Denial of Service vulnerability in the Kubernetes kubelet component, where unauthenticated requests to the read-only HTTP endpoint can fill up node disk space via the checkpoint API, potentially leading to node unavailability.</p> <p>Mitigation: Argo service does not directly interact with kubelet endpoints. It communicates exclusively with the Kubernetes API server (kube-apiserver) to manage the desired state of applications. Therefore, the service does not make any requests to kubelet's read-only or write endpoints, nor does it depend on this functionality for its operation. As a result, this vulnerability does not directly impact the functionality.</p>	
argo-rollouts	v1.7.2-cap-CR-28008	CVE-2024-9042	This vulnerability is not applicable to Argo services, as it cannot be deployed on Windows nodes. The service runs exclusively on Linux-based nodes, and the affected /logs/query API endpoint is only present and exploitable on Windows nodes. Therefore, this issue does not pose any risk to Argo environments.	
argo-events	v1.9.2-cap-CR-29689	CVE-2025-30204	The argo-events component includes github.com/golang-jwt/jwt as a transitive dependency through the module github.com/Azure/azure-sdk-for-go/sdk/storage/azqueue. This library is not used directly by our service logic, and no JWT token parsing or validation is performed via this path. Therefore, any potential issues or vulnerabilities in github.com/golang-jwt/jwt do not affect the behavior or security of our service.	

Onprem Version 2.8.6 - Published 12 June 2025			
Image	Tag	CVE	Mitigation
argo-platform-abac	1.3525.0-onprem-d01c752	CVE-2023-26108	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.
argo-platform-analytics-reporter	1.3525.0-onprem-d01c752	CVE-2023-26108	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.
argo-platform-api-events	1.3525.0-onprem-d01c752	CVE-2023-26108	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.
argo-platform-api-graphql	1.3525.0-onprem-d01c752	CVE-2023-26108	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.
argo-platform-api-graphql	1.3525.0-onprem-d01c752	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.
argo-platform-audit	1.3525.0-onprem-d01c752	CVE-2023-26108	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.
argo-platform-broadcaster	1.3525.0-onprem-d01c752	CVE-2025-25288	Vulnerability nested in package @octokit/rest. It won't affect the service because the package added long time ago and its usage was deleted without cleaning dependency list. It will be deleted in next release.
argo-platform-broadcaster	1.3525.0-onprem-d01c752	CVE-2023-26108	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.
argo-platform-broadcaster	1.3525.0-onprem-d01c752	CVE-2025-25290	Vulnerability nested in package @octokit/rest. It won't affect the service because the package added long time ago and its usage was deleted without cleaning dependency list. It will be deleted in next release.
argo-platform-broadcaster	1.3525.0-onprem-d01c752	CVE-2025-25289	Vulnerability nested in package @octokit/rest. It won't affect the service because the package added long time ago and its usage was deleted without cleaning dependency list. It will be deleted in next release.
argo-platform-cron-executor	1.3525.0-onprem-d01c752	CVE-2025-25289	Vulnerability nested in package @octokit/rest. It won't affect the service because the package added long time ago and its usage was deleted without cleaning dependency list. It will be deleted in next release.
argo-platform-cron-executor	1.3525.0-onprem-d01c752	CVE-2025-25288	Vulnerability nested in package @octokit/rest. It won't affect the service because the package added long time ago and its usage was deleted without cleaning dependency list. It will be deleted in next release.
argo-platform-cron-executor	1.3525.0-onprem-d01c752	CVE-2025-25290	Vulnerability nested in package @octokit/rest. It won't affect the service because the package added long time ago and its usage was deleted without cleaning dependency list. It will be deleted in next release.
argo-platform-cron-executor	1.3525.0-onprem-d01c752	CVE-2023-26108	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.
argo-platform-event-handler	1.3525.0-onprem-d01c752	CVE-2023-26108	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.
argo-platform-promotion-orchestrator	1.3525.0-onprem-d01c752	CVE-2023-26108	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.
argo-platform-promotion-orchestrator	1.3525.0-onprem-d01c752	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.
cf-api	21.279.5	CVE-2024-11023	CVE-2024-11023: Firebase JavaScript SDK utilizes a "FIREBASE_DEFAULTS" cookie to store configuration data, including an "_authTokenSyncURL" field used 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 an actor to capture user session data transmitted by the SDK.
cf-api	21.279.5	CVE-2020-36604	As it stems from the description, this issue affects only browser usage of Firebase SDK, and is not relevant for server-side JS because of absence of cookies per session.
cf-api	21.279.5	CVE-2022-23539	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.
cf-api	21.279.5	CVE-2021-3377	We do not configure the jsonwebtoken library to use custom key types or algorithms, thus the default settings are used. As a result, the vulnerability does not affect our application since it only impacts configurations using invalid key types / algorithm combinations, which we do not utilize.
cf-broadcaster	1.13.0	CVE-2020-36604	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 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.
cf-deploy-kubernetes	16.2.6	CVE-2023-42366	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.
cf-deploy-kubernetes	16.2.6	CVE-2022-48174	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-2023-42364	CVE-2022-48174 describes a stack overflow vulnerability in the ash shell implementation (ash.c) in BusyBox versions prior to 1.35. This vulnerability may allow an attacker to achieve arbitrary code execution via specially crafted shell input.
cf-deploy-kubernetes	16.2.6	CVE-2023-42365	Our system is not affected by this vulnerability, as we do not use the ash shell or any BusyBox shell components in our software. As such, the CVE is not applicable to our product or deployment configuration.
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.

Onprem Version 2.8.6 - Published 12 June 2025			
Image	Tag	CVE	Mitigation
cf-docker-puller	8.0.20	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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-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-2023-42366	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-2023-42365	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-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
cf-git-cloner	10.2.0	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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-2022-48174	CVE-2022-48174 describes a stack overflow vulnerability in the ash shell implementation (<code>ash.c</code>) in BusyBox versions prior to 1.35. This vulnerability may allow an attacker to achieve arbitrary code execution via specially crafted shell input. Our system is not affected by this vulnerability, as we do not use the ash shell or any BusyBox shell components in our software. As such, the CVE is not applicable to our product or deployment configuration.
cf-platform-analytics	0.50.2	CVE-2022-36313	The vulnerable package "file-type" is nested in "decompress" package.
cf-platform-analytics	0.50.2	CVE-2024-27088	The CVE-2022-36313 vulnerability relates specifically to .mkv file type handling. The decompress package utilizes file-type exclusively for detecting types such as tar, tarbz2, targz, and zip. Therefore, the service is not affected by this vulnerability.
cf-platform-analytics	0.50.2	CVE-2020-36604	Our approach mitigates the vulnerability by enforcing simplified function naming conventions and prioritizing updated dependencies that prevent script stalls caused by complex function declarations
cf-platform-analytics	0.50.2	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.
charts-manager	1.23.2	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.
consul	1.21.1-debian-12-r3	PRISMA-2023-0056	latest upstream version
context-manager	2.34.3	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.
engine	1.178.0	CVE-2024-11023	CVE-2024-11023: Firebase JavaScript SDK utilizes a "FIREBASE_DEFAULTS" cookie to store configuration data, including an "_authTokenSyncURL" field used 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 an actor to capture user session data transmitted by the SDK.
engine	1.178.0	CVE-2020-36604	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 session
engine	1.178.0	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.
engine	1.178.0	CVE-2024-28176	Service utilizes the jose module as nested module in jsonwebtoken. 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
engine	1.178.0	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.
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.
pikolo	0.14.3	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.

Onprem Version 2.8.6 - Published 12 June 2025			
Image	Tag	CVE	Mitigation
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.
pikolo	0.14.3	CVE-2022-48174	CVE-2022-48174 describes a stack overflow vulnerability in the ash shell implementation (ash.c) in BusyBox versions prior to 1.35. This vulnerability may allow an attacker to achieve arbitrary code execution via specially crafted shell input. Our system is not affected by this vulnerability, as we do not use the ash shell or any BusyBox shell components in our software. As such, the CVE is not applicable to our product or deployment configuration.
pikolo	0.14.3	CVE-2022-30065	The awk package is a nested package within BusyBox, and the vulnerability is associated with the use of awk. However, our service and its components do not utilize awk in any capacity. Therefore, this vulnerability does not impact the functionality or security of our service.
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.
pipeline-manager	3.139.3	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.
runtime-environment-manager	3.41.2	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.
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.

CVE Mitigations from V2.2.5 to V2.6.9			
Onprem version 2.7.13 - Published 20 May 2025			
Image	Tag	CVE	Mitigation
argo-platform-api-graphql	1.3344.2-onprem-3feba0e	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.
argo-platform-api-graphql	1.3344.2-onprem-3feba0e	CVE-2023-26108	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.
argo-platform-api-graphql	1.3344.2-onprem-3feba0e	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.
argo-platform-api-graphql	1.3344.2-onprem-3feba0e	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.
argo-platform-api-graphql	1.3344.2-onprem-3feba0e	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.
argo-platform-api-graphql	1.3344.2-onprem-3feba0e	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
engine	1.177.7	CVE-2024-11023	CVE-2024-11023: Firebase JavaScript SDK utilizes a "FIREBASE_DEFAULTS" cookie to store configuration data, including an "_authTokenSyncURL" field used 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 an actor to capture user session data transmitted by the SDK.
engine	1.177.7		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.
argo-platform-audit	1.3344.2-onprem-3feba0e	CVE-2023-26108	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.
argo-platform-audit	1.3344.2-onprem-3feba0e	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.
argo-platform-audit	1.3344.2-onprem-3feba0e	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.
argo-platform-audit	1.3344.2-onprem-3feba0e	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
pipeline-manager	3.138.5	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.
cf-debugger	1.3.7	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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-api	21.274.15	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.
cf-api	21.274.15	CVE-2022-23539	We do not configure the jsonwebtoken library to use custom key types or algorithms, thus the default settings are used. As a result, the vulnerability does not affect our application since it only impacts configurations using invalid key types / algorithm combinations, which we do not utilize.
consul	1.21.0-debian-12-r1	PRISMA-2023-0056	Latest upstream version
argo-events	v1.9.2-cap-CR-28072	CVE-2025-21613	The vulnerability in go-git allows argument injection via the file:// protocol, potentially enabling attackers to manipulate git-upload-pack parameters and execute unintended commands. Mitigation: Argo Events is not affected because it does not use the file:// protocol or local Git repositories. It interacts with remote repositories via HTTP/S or SSH webhooks and does not execute git-upload-pack directly.
engine	1.177.7	CVE-2024-28176	Service utilizes the jose module as nested module in jsonwebtoken. 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
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-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-2022-33987	Dependency is located in NPM, and not related to or used in app/package/run.

CVE Mitigations from V2.2.5 to V2.6.9			
Onprem version 2.7.13 - Published 20 May 2025			
Image	Tag	CVE	Mitigation
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.
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.
argo-platform-abac	1.3344.2-onprem-3feba0e	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.
argo-platform-event-handler	1.3344.2-onprem-3feba0e	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.
argo-platform-event-handler	1.3344.2-onprem-3feba0e	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.
argo-platform-event-handler	1.3344.2-onprem-3feba0e	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.
argo-platform-event-handler	1.3344.2-onprem-3feba0e	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
cf-platform-analytics	0.49.87	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
argo-platform-api-events	1.3344.2-onprem-3feba0e	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-api	21.274.15	CVE-2021-3377	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 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.
argo-platform-abac	1.3344.2-onprem-3feba0e	CVE-2023-26108	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.
argo-platform-abac	1.3344.2-onprem-3feba0e	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.
argo-platform-abac	1.3344.2-onprem-3feba0e	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.
argo-platform-abac	1.3344.2-onprem-3feba0e	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
argo-platform-cron-executor	1.3344.2-onprem-3feba0e	CVE-2023-26108	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.
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-2023-42365	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-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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-2023-42365	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-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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-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.
argo-platform-promotion-orchestrator	1.3344.2-onprem-3feba0e	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.
argo-platform-promotion-orchestrator	1.3344.2-onprem-3feba0e	CVE-2023-26108	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.
argo-platform-promotion-orchestrator	1.3344.2-onprem-3feba0e	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.
argo-platform-promotion-orchestrator	1.3344.2-onprem-3feba0e	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.

CVE Mitigations from V2.2.5 to V2.6.9			
Onprem version 2.7.13 - Published 20 May 2025			
Image	Tag	CVE	Mitigation
argo-platform-promotion-orchestrator	1.3344.2-onprem-3feba0e	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.
argo-platform-promotion-orchestrator	1.3344.2-onprem-3feba0e	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
cf-platform-analytics	0.49.87	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.
argo-platform-cron-executor	1.3344.2-onprem-3feba0e	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.
argo-platform-cron-executor	1.3344.2-onprem-3feba0e	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.
argo-platform-cron-executor	1.3344.2-onprem-3feba0e	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.
argo-platform-cron-executor	1.3344.2-onprem-3feba0e	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
cf-docker-builder	1.4.4	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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-2022-48174	CVE-2022-48174 describes a stack overflow vulnerability in the ash shell implementation (ash.c) in BusyBox versions prior to 1.35. This vulnerability may allow an attacker to achieve arbitrary code execution via specially crafted shell input. Our system is not affected by this vulnerability, as we do not use the ash shell or any BusyBox shell components in our software. As such, the CVE is not applicable to our product or deployment configuration.
cf-docker-builder	1.4.4	CVE-2022-30065	The awk package is a nested package within BusyBox, and the vulnerability is associated with the use of awk. However, our service and its components do not utilize awk in any capacity. Therefore, this vulnerability does not impact the functionality or security of our service.
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-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
pikolo	0.14.3	CVE-2022-48174	CVE-2022-48174 describes a stack overflow vulnerability in the ash shell implementation (ash.c) in BusyBox versions prior to 1.35. This vulnerability may allow an attacker to achieve arbitrary code execution via specially crafted shell input. Our system is not affected by this vulnerability, as we do not use the ash shell or any BusyBox shell components in our software. As such, the CVE is not applicable to our product or deployment configuration.
pikolo	0.14.3	CVE-2022-30065	The awk package is a nested package within BusyBox, and the vulnerability is associated with the use of awk. However, our service and its components do not utilize awk in any capacity. Therefore, this vulnerability does not impact the functionality or security of our service.
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.
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.
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.
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.
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.
context-manager	2.33.7	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.

CVE Mitigations from V2.2.5 to V2.6.9			
Onprem version 2.7.13 - Published 20 May 2025			
Image	Tag	CVE	Mitigation
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.
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.
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.
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.
cf-ui	14.97.51	CVE-2023-42363	The vulnerability affects the xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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-2022-48174	CVE-2022-48174 describes a stack overflow vulnerability in the ash shell implementation (ash.c) in BusyBox versions prior to 1.35. This vulnerability may allow an attacker to achieve arbitrary code execution via specially crafted shell input. Our system is not affected by this vulnerability, as we do not use the ash shell or any BusyBox shell components in our software. As such, the CVE is not applicable to our product or deployment configuration.
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.
argo-platform-api-events	1.3344.2-onprem-3feba0e	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.
argo-platform-api-events	1.3344.2-onprem-3feba0e	CVE-2023-42363	The vulnerability affects the xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
argo-platform-ui	1.3344.2-onprem-3feba0e	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.
argo-platform-broadcaster	1.3344.2-onprem-3feba0e	CVE-2023-26108	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.
argo-platform-event-handler	1.3344.2-onprem-3feba0e	CVE-2023-26108	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.
argo-platform-broadcaster	1.3344.2-onprem-3feba0e	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.
argo-platform-broadcaster	1.3344.2-onprem-3feba0e	CVE-2023-42363	The vulnerability affects the xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
argo-platform-ui	1.3344.2-onprem-3feba0e	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.
argo-platform-ui	1.3344.2-onprem-3feba0e	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.
argo-platform-ui	1.3344.2-onprem-3feba0e	CVE-2023-42363	The vulnerability affects the xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
cf-git-cloner	10.2.0	CVE-2023-42363	The vulnerability affects the xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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-2022-48174	CVE-2022-48174 describes a stack overflow vulnerability in the ash shell implementation (ash.c) in BusyBox versions prior to 1.35. This vulnerability may allow an attacker to achieve arbitrary code execution via specially crafted shell input. Our system is not affected by this vulnerability, as we do not use the ash shell or any BusyBox shell components in our software. As such, the CVE is not applicable to our product or deployment configuration.
cf-docker-builder	1.4.4	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.

Onprem version 2.7.13 - Published 20 May 2025			
Image	Tag	CVE	Mitigation
argo-platform-audit	1.3344.2-onprem-3feba0e	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.
argo-platform-api-events	1.3344.2-onprem-3feba0e	CVE-2023-26108	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.
argo-platform-api-events	1.3344.2-onprem-3feba0e	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-2023-42364	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.
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.
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.
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.
runtime-environment-manager	3.39.4	CVE-2023-42363	The vulnerability affects the xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
argo-platform-broadcaster	1.3344.2-onprem-3feba0e	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.
argo-platform-broadcaster	1.3344.2-onprem-3feba0e	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.
chartmuseum	8795e993	CVE-2023-42363	The vulnerability affects the xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
argo-platform-analytics-reporter	1.3344.2-onprem-3feba0e	CVE-2023-26108	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.
argo-platform-analytics-reporter	1.3344.2-onprem-3feba0e	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.
argo-platform-analytics-reporter	1.3344.2-onprem-3feba0e	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.
argo-platform-analytics-reporter	1.3344.2-onprem-3feba0e	CVE-2023-42363	The vulnerability affects the xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
argo-platform-analytics-reporter	1.3344.2-onprem-3feba0e	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.
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.

CVE Mitigations from V2.2.5 to V2.6.9			
Onprem version 2.7.12 - Published 20 May 2025			
Image	Tag	CVE	Mitigation
argo-platform-analytics-reporter	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.
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.
argo-platform-analytics-reporter	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affecting BusyBox and the xsprintf function does not affect the security of environments that use Node.js without using BusyBox directly
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.
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.
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.
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.
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.
argo-platform-ui	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
cf-debugger	1.3.7	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
cf-ui	14.97.51	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
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.
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
cf-docker-puller	8.0.20	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.

CVE Mitigations from V2.2.5 to V2.6.9			
Onprem version 2.7.12 - Published 20 May 2025			
Image	Tag	CVE	Mitigation
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 affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
context-manager	2.33.7	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
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.
argo-platform-broadcaster	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.
argo-platform-broadcaster	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.
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.
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.
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.
argo-platform-broadcaster	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
cf-git-cloner	10.2.0	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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 affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
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.
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.

CVE Mitigations from V2.2.5 to V2.6.9			
Onprem version 2.7.12 - Published 20 May 2025			
Image	Tag	CVE	Mitigation
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.
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.
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
argo-platform-cron-executor	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.
argo-platform-cron-executor	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
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.
cf-docker-builder	1.4.4	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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	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-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.
argo-platform-event-handler	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.
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.
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.
argo-platform-event-handler	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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 affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
argo-platform-api-events	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.

CVE Mitigations from V2.2.5 to V2.6.9			
Onprem version 2.7.12 - Published 20 May 2025			
Image	Tag	CVE	Mitigation
argo-platform-api-events	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
pikolo	0.14.3	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
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.
docker.io/bitnami/consul	1.21.0-debian-12-r1	PRISMA-2023-0056	Latest upstream version
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.
chartmuseum	8795e993	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
argo-platform-api-graphql	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.
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.
argo-platform-api-graphql	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
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.
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.
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.
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.
runtime-environment-manager	3.39.4	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
argo-platform-abac	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.
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.
argo-platform-abac	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affects the <code>xasprintf</code> function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
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.

CVE Mitigations from V2.2.5 to V2.6.9			
Onprem version 2.7.12 - Published 20 May 2025			
Image	Tag	CVE	Mitigation
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 an 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 to or used in 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 jsonwebtoken. 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
argo-platform-promotion-orchestrator	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.
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.
argo-platform-promotion-orchestrator	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.
argo-platform-promotion-orchestrator	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
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.
argo-platform-audit	1.3344.0-onprem-5c8af92	CVE-2023-26108	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.
argo-platform-audit	1.3344.0-onprem-5c8af92	CVE-2023-42363	The vulnerability affects the xsprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
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.
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.
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.