CVE Mitigations from V2.2.5 to V2.6.9
Version 2.7.13 – Published 16 May 2025

Image	Tag	CVE	Mitigation
Image: argo-events Count: 1		Unique: 1	
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.
Image: argo-platform-abac Count: 5		Unique: 5	
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-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 xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.
Image: argo-platform-analytics-reporter		Unique: 5	
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.
Image: argo-platform-api-events Count: 5		Unique: 5	
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.
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.
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.
Image: argo-platform-api-graphql		Unique: 6	
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 xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.

Image: argo-platform-audit
Count: 5   Unique: 5

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 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-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.

Image: argo-platform-broadcaster
Count: 5   Unique: 5

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-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-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.

Image: argo-platform-cron-executor
Count: 5   Unique: 5

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.
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 xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.

Image: argo-platform-event-handler
Count: 5   Unique: 5

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 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-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.

Image: argo-platform-promotion-orchestrator
Count: 6   Unique: 6

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.
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 xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.

Image: argo-platform-ui
Count: 4   Unique: 4

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-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.

Image: cf-api
Count: 3   Unique: 3

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.
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.

Image: cf-broadcaster
Count: 1   Unique: 1

cf-broadcaster	1.13.0	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.

Image: cf-debugger   Unique: 4

cf-debugger	1.3.7	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-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-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.

Image: cf-deploy-kubernetes
Count: 5   Unique: 5

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.

Image: cf-docker-builder
Count: 7   Unique: 7

cf-docker-builder	1.4.4	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.
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.
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.
Image: cf-docker-puller Count: 4		Unique: 4	
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 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-docker-puller	8.0.20	CVE-2023-42364	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: cf-docker-pusher		Unique: 4	
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 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-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.
Image: cf-docker-tag-pusher Count: 4		Unique: 4	
cf-docker-tag-pusher	1.3.15	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
cf-docker-tag-pusher	1.3.15	CVE-2023-42363	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-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.
Image: cf-git-cloner Count: 5		Unique: 5	
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 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.
Image: cf-platform-analytics Count: 2		Unique: 2	
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
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.
Image: cf-ui Count: 4		Unique: 4	
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.
Image: chartmuseum Count: 4		Unique: 4	
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.
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.
Image: charts-manager Count: 1		Unique: 1	
charts-manager	1.22.3	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.
Image: consul Count: 1		Unique: 1	
consul	1.21.0-debian-12-r1	PRISMA-2023-0056	Latest upstream version
Image: context-manager Count: 5		Unique: 5	
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 xasprintf 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-2023-42366	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
Image: engine		Unique: 5	

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 am actor to capture user session data transmitted by the SDK. As it stems from the description, this issue affects only browser usage of Firebase SDK, and not relevant for server-side JS because of absence of cookies per se.
engine	1.177.7	CVE-2024-28176	Service utilizes the jose module as nested module in jsonwebtoket. But does not perform any operation of unpacking decrypted text, and we don't use JWE at all. This vulnerability will not impact our service
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.
Image: gitops-dashboard-manager Count: 1		Unique: 1	
gitops-dashboard-manager	1.14.22	CVE-2020-36604	Hoek package is used only within the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in very few Joi functions. Our risk assessment confirms that vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.
Image: pikolo Count: 7		Unique: 7	
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 xasprintf 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.
Image: pipeline-manager Count: 1		Unique: 1	
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.
Image: runtime-environment-manager Count: 5		Unique: 5	
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.
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.
Image: tasker-kubernetes Count: 1		Unique: 1	

| 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. |

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 xasprintf 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 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-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 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-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 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-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 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-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.

Version 2.7.12 – Published 20 May 2025

Image	Tag	CVE	Mitigation
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.
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 xasprintf 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 xasprintf 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 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-2023-42364	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 xasprintf function in BusyBox. It does not impact the security of environments using Node.js, provided BusyBox is not used directly in those environments.

Version 2.7.12 – Published 20 May 2025

Image	Tag	CVE	Mitigation
cf-git-cloner	10.2.0	CVE-2023-42365	Service mitigates potential vulnerabilities by not accepting and utilizing user input in operations involving text files and the AWK utility. This approach minimizes risks associated with external data manipulation, ensuring a more secure handling of file operations within our Node.js environment.
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.
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 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-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 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-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.

Version 2.7.12 – Published 20 May 2025

Image	Tag	CVE	Mitigation
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 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-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 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-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.
argo-platform-api-events	1.3344.0-onprem-5c8af92	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.
pikolo	0.14.3	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-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 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.
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 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-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.

Version 2.7.12 – Published 20 May 2025

Image	Tag	CVE	Mitigation
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 xasprintf 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 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-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.
engine	1.177.7	CVE-2024-11023	Firebase JavaScript SDK utilizes a "FIREBASE_DEFAULTS" cookie to store configuration data, including an "_authTokenSyncURL" field for session synchronization. If this cookie field is preset via an attacker by any other method, the attacker can manipulate the "_authTokenSyncURL" to point to their own server and it would allow am actor to capture user session data transmitted by the SDK. As it stems from the description, this issue affects only browser usage of Firebase SDK, and not relevant for server-side JS because of absence of cookies per se.
engine	1.177.7	CVE-2022-33987	Dependency is located in NPM, and not related 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 jsonwebtoket. But does not perform any operation of unpacking decrypted text, and we don't use JWE at all. This vulnerability will not impact our service
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 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-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.

[CVE Mitigations from V2.2.5 to V2.6.9](#)

Version 2.7.12 – Published 20 May 2025

Image	Tag	CVE	Mitigation
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 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-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.

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.

Service mitigates potential vulnerabilities by refusing to accept user input and abstaining from utilizing it 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.

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.

Hoek package is used only inside the Joi package which is responsible for data validation using schema. Vulnerable "clone" function is used in a very small amount of Joi functions. Our risk assessment confirms that vulnerable hoek method "clone" does not affect any codefresh business logic by usage of Joi functions that we exploit in that business logic.

dependency is located in "npm" and not related/used to app package/run.

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.

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.

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.

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 the vulnerable Hoek "clone"method does not affect any Codefresh business logic in the Joi functions where we exploit the business logic.

Dependency is located in NPM, and not related to or used in app/package/run.