

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

Version 2.7.12 - Published 20 May 2025

Image	Tag	CVE	Mitigation
Image: argo-platform-abac Count: 5			
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.
Image: argo-platform-analytics-reporter Count: 5			
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.
Image: argo-platform-api-events Count: 5			
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.
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.
Image: argo-platform-api-graphql Count: 6			
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.

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

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.
Image: argo-platform-audit Count: 5			
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.
Image: argo-platform-broadcaster Count: 6			
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.
Image: argo-platform-cron-executor Count: 5			
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.
Image: argo-platform-event-handler			
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.

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

Version 2.7.12 - Published 20 May 2025

Image	Tag	CVE	Mitigation
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.
Image: argo-platform-promotion-orchestrator Count: 7			
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.
Image: argo-platform-ui Count: 4			
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.
Image: cf-broadcaster Count: 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 Count: 4			
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.
Image: cf-deploy-kubernetes Count: 4			

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

Version 2.7.12 - Published 20 May 2025

Image	Tag	CVE	Mitigation
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.
Image: cf-docker-builder Count: 6			
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.
Image: cf-docker-puller Count: 4			
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.
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.
Image: cf-docker-pusher Count: 4			
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.
Image: cf-docker-tag-pusher Count: 4			

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

Version 2.7.12 - Published 20 May 2025

Image	Tag	CVE	Mitigation
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.
Image: cf-git-cloner Count: 7			
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.
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.
Image: cf-platform-analytics			
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
Image: cf-ui Count: 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-2023-42363	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.
Image: chartmuseum Count: 5			
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-2023-42364	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.

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

Version 2.7.12 - Published 20 May 2025

Image	Tag	CVE	Mitigation
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.
Image: charts-manager Count: 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: context-manager Count: 6			
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.
Image: docker.io/bitnami/consul Count: 1			
docker.io/bitnami/consul	1.21.0-debian-12-r1	PRISMA-2023-0056	Latest upstream version
Image: engine Count: 5			
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	Firestore 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 Firestore 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
Image: gitops-dashboard-manager Count: 1			

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

Version 2.7.12 - 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.
Image: pikolo Count: 6			
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	<code>cf-docker-builder</code>
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.
Image: runtime-environment-manager Count: 5			
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.
Image: tasker-kubernetes Count: 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.