1 Finding Details

Low

Information Disclosure in Grafana

Overall Risk	Low	**Finding ID**	NCC-E004027-INPT-DMA
Impact	Low	**Component**	Prod INPT
Exploitability	High	**Category**	Error Reporting
		Status	New

Impact

The Grafana application discloses its absolute path when an attacker accesses a non-existent URL. Although this issue itself is not very serious, it can be chained with exploitation of other vulnerabilities such as the path traversal vulnerability documented in finding finding "Grafana 8.2.1 Path Traversal Vulnerability (CVE-2021-43798)".

Description

Multiple servers are running Grafana applications, and all instances of the Grafana application display error message when an attacker accesses a non-existent URL. The error message reveals the absolute path of the Grafana application, and if other vulnerabilities such as path traversal vulnerability do exist, error messages can be used to verify the existence of a specific file.

Recommendation

The application should trap all errors and present a generic error message to the user. Error details should be logged in the back end to a location not accessible from the external network.
Debugging and development functionality should not be enabled in production services. Ensure this functionality is completely disabled through the relevant configuration option.
Ensure responses do not contain sensitive information by stripping the disclosed information from the noted responses. If there is a risk of information being disclosed in multiple locations, consider creating an abstraction on data access that automatically strips sensitive data.

Reproduction Steps

1. Access https://host/public/plugins/alertlist/etc/passwd.
2. Observe the error message displayed in response.

Location

- https://10.25.40.218/
- https://10.25.41.160/
- https://10.25.40.53/
- https://10.25.41.58/
- https://10.25.41.91/
- https://10.25.40.141/