Hive Pro

THREAT ADVISORY

Grafana releases an emergency patch for a Zero-Day vulnerability

TA202156

Threat Level AMBER

Publish Date – Dec 8, 2021

Grafana, a database analyzing, and monitoring tool used by major companies has been affected by a high severe zero-day vulnerability.

CVE-2021-43798 is a path traversal vulnerability that allows an attacker to traverse outside the Grafana folder and remotely access restricted files.

Grafana comes with some pre-installed plugins like graph, MySQL etc. The vulnerability affects the URL path of the plugins. So, all the Grafana instances are vulnerable. The vulnerable URL path is: <grafana_host_url>/public/plugins/<“plugin-id”> where <“plugin-id”> is the plugin ID for any installed plugin.

This vulnerability affects versions 8.0.0-beta1 through 8.3.0. and has been fixed in versions 8.3.1, 8.2.7, 8.1.8, and 8.0.7. An emergency patch has been released by Grafana Labs after exploits started circulating over Twitter and GitHub. Grafana has advised to update the affected systems as soon as possible. However, the organizations that cannot upgrade their systems can run a reverse proxy in front of Grafana that normalizes the PATH of the request which will eliminate this flaw.

Vulnerability Detail

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-43798	Grafana versions 8.0.0-beta1 to 8.3.0	cpe:2.3:a:grafana:grafana:8.0:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.0.1:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.0.2:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.0.3:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.0.4:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.0.5:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.0.6:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.1:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.1.0:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.1.1:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.1.2:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.1.3:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.1.4:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.1.5:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.1.6:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.1.7:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.2:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.2.0:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.2.1:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.2.2:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.2.3:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.2.4:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.2.5:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.2.6:*:*:*:*:*:*:*, cpe:2.3:a:grafana:grafana:8.3:*:*:*:*:*:*:*	Grafana Path Traversal Vulnerability	CWE-22

Patch Link

https://grafana.com/blog/2021/12/07/grafana-8.3.1-8.2.7-8.1.8-and-8.0.7-released-with-high-severity-security-fix/

Reference

https://www.bleepingcomputer.com/news/security/grafana-fixes-zero-day-vulnerability-after-exploits-spread-over-twitter/