Grafana Labs

Unauthenticated DoS in avatar cache in Grafana

High

Advisory ID:	CVE-2026-21720
Published:	2026-01-27
Product:	Grafana
CVSS Score:	7.5
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Fixed Versions:	>=12.3.0 <12.3.1+security-01 >=12.2.0 <12.2.3+security-01 >=12.1.0 <12.1.5+security-01 >=12.0.0 <12.0.8+security-01 >=3.0.0 <11.6.9+security-01

Summary

Grafana is an open-source platform for monitoring and observability. The platform supports users having their own avatars, which can be sourced from the Gravatar service API. This uses a cache, to ensure that we don't overload the service.

If these requests time out after 3 seconds, a Goroutine is left running forever. This can cause a denial of service (DoS) if an attacker repeats these requests.

This bug was reported by sam18191 via our bug bounty program.