Executive Situation Report | Surge in Coordinated Grafana Exploitation Attempts

Key Judgments & Evidence

1. **On 28 September, a single threat actor — or several actors using the same exploit kit and target set — attempted to exploit Grafana at scale using an old vulnerability.**
   - GreyNoise observed 110 unique IPs attempting to exploit Grafana assets leveraging CVE-2021-43798, a sharp increase from the near-zero baseline in prior weeks.
   - IPs from each source country targeted the same three destination countries.
   - The top three TCP fingerprints all mapped to the same three destinations, suggesting a single operator or shared exploit kit/target set.
2. **Successful exploitation allows an attacker to read Grafana/system files, enabling account takeover and lateral access.**
   - CVE-2021-43798 is a path traversal vulnerability that permits arbitrary file reads including API keys, credentials, and dashboard data.
3. **Exploitation attempts disproportionately focused on U.S.-based assets and originated largely from APAC-based IPs.**
   - U.S., Slovakia, and Taiwan were the sole target countries.
   - The top three source countries were Bangladesh (107 IPs), China (2 IPs), and Germany (1 IP).
   - Of the 107 Bangladesh-based IPs, 105 targeted U.S. endpoints.

Top 3 Source Countries:	BANGLADESH (97%) CHINA (2%) GERMANY (1%)
Top 3 Target Countries:	UNITED STATES (83%) SLOVAKIA (8%) TAIWAN (8%)

Strategic Threat Context

GLOBAL EXPLOITATION:	VULNERABILITY REUSE & TOOLKITS:	EXPLOIT CHAINS & RECONNAISSANCE:
Grafana path traversal and related vulnerabilities have been leveraged in large-scale SSRF / exploit waves targeting many IPs and software ecosystems.	Grafana flaws (e.g., CVE-2025-6023) are being actively researched and weaponized for account takeovers and integrated into attacker tool sets.	In advisories and analyses, Grafana vulnerabilities show up in reconnaissance stages of multi-step exploit chains (such as SSRF campaigns).

Recommended Actions

> Block the 110 malicious IPs observed on 28 September.

> Confirm Grafana instances are patched against CVE-2021-43798.

> Review logs for evidence of traversal requests and ensure no sensitive files were returned.

Implications

> **Old flaws remain dangerous:** CVE-2021-43798 continues to be exploited at scale, highlighting risk from unpatched Grafana.

> **Shared tooling drives speed:** Convergent geo/fingerprint patterns suggest exploit kits or shared target lists.

> **U.S. assets prioritized:** Majority of observed traffic was directed at U.S. endpoints.

Threat Actor Activity (Past 90 Days)

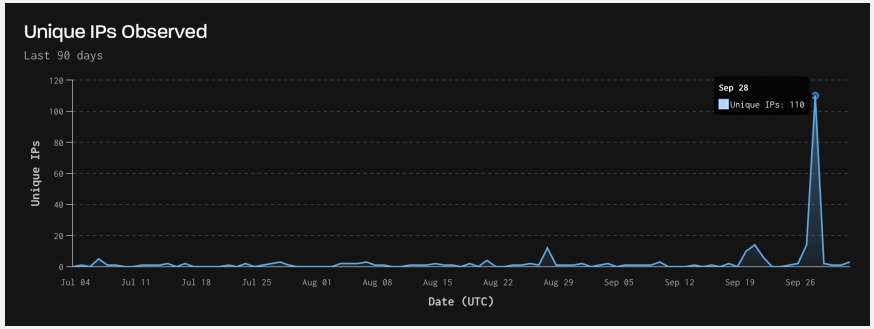

Figure 1. Grafana path traversal activity (Source: GreyNoise Global Observation Grid (GOG))

Peak Activity:
110 unique IPs (28 September 2025)

Baseline: ~5 IPs daily

Percentage Increase: ~2,000%

Significant spike in exploitation attempts against Grafana endpoints.

Data from: GreyNoise "Grafana Path Traversal Attempt" tag

Timeframe: 28 September 2025
Source: GreyNoise Intelligence

Original GreyNoise Analysis