Threat Intelligence & CVE Analysis

Christopher D. Contreras

California State University, Fullerton

College of Engineering & Computer Science

CPSC 253: Cybersecurity Foundation and Principles

Professor Michael Franklin

March 12, 2025

Table of Contents

Executive Summary

The purpose of this report is to analyze the common vulnerability and exposure (CVE) found in Grafana, which is an open-source platform used for data analytics and visualization. The report details specific vulnerabilities allowing unauthorized deletion of the dashboard snapshot by users who did not have the right permissions. While the snapshot flaw affects snapshot data rather than very sensitive data, it still poses a risk of undermining user confidence in the platform. Attack vectors for exploiting the vulnerability involve getting the snapshot key, typically shared through the dashboard or email. Successful exploitation could disrupt the platform's integrity, and it is recommended that any organization that is using a version post-10.4.0 should update their system. This vulnerability showcases a moderate severity score of 6.5 due to the insufficient permission check during the snapshot deletion. Moreover, this analysis highlights a correlation between a broader risk that was shown by an incident in the CircleCI breach, where attackers similarly exploit authorization through stolen tokens. Therefore, this report strongly recommends implementing rigorous patch management, regular security audits, and enhanced threat intelligence processes. The measures are essential to mitigate vulnerabilities and proactively maintain security against cybersecurity threats.

CVE Analysis

Overview

This CVE analysis shows the vulnerability found in the Grafana platform, identified as CVE-2024-1313. Grafana is an open-source resource that uses data for visualization and analytics, allowing users to understand their data. In a usual scenario, the user must possess the correct permission to modify and remove dashboard snapshots. However, the CVE file that Grafana has created states, "It is possible for a user in a different organization from the owner of a snapshot to bypass authorization and delete a snapshot by issuing a DELETE request to /api/snapshots/<key> using its view key" (Grafana Labs, 2024). Grafana is a platform for 25 million users and used widely throughout the world displaying the potential impact it could have.

Technical Impact

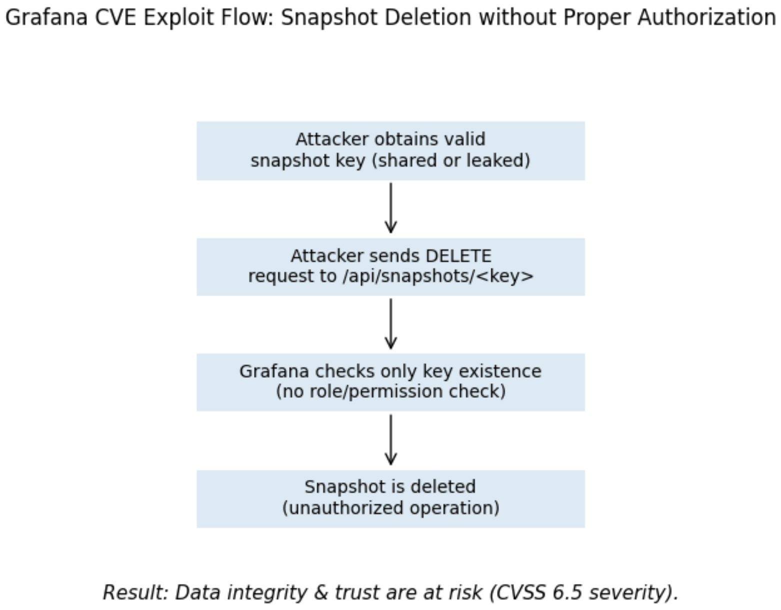
This problem stems from the Grafana platform as it allows users to delete a snapshot without having access when it is only intended to be viewed. Instead of checking that the user has the correct authorization level, the system will validate a user through the existence of a snapshot key, which assumes that the user is the owner of the set information. Although the Common Vulnerability Scoring System rated this at 6.5, it creates a source for threat agents to misuse the dashboard since it serves as an asset. The Grafana flaw highlights a serious risk to data integrity and operations, as the organization relies on critical data for monitoring and reporting. Therefore, this lack of integrity in the platform can lead to trust issues with the platform as it fails to meet the proper security standards.

Attack Vectors

Another aspect of understanding this vulnerability is examining how attack vectors and potential exploitation methods can be used if an attacker had infiltrated this system and software.

First, the hacker would have to obtain a valid snapshot key since snapshots are shared in places like dashboards or emails. Once they have the key, the attacker can issue the delete request for the snapshot, which Grafana will interpret as a correct request. With all this being said, there is a higher chance of this attack occurring if these keys are disturbed all over the platform. This is extremely difficult to do, however, with the right amount of luck or accidental leak, an attacker can receive all the information needed to access something that is meant to be protected and secured.

Fig 1


Grafana CVE Exploit Flow: Snapshot Deletion without Proper Authorization
Attacker obtains valid snapshot key (shared or leaked)
Attacker sends DELETE request to /api/snapshots/<key>
Grafana checks only key existence (no role/permission check)
Snapshot is deleted (unauthorized operation)
Result: Data integrity & trust are at risk (CVSS 6.5 severity).

Affected Versions

Furthermore, when these snapshot attacks occur, the CVE states, "Grafana Labs would like to thank Ravid Mazon and Jay Chen of Palo Alto Research for discovering and disclosing this vulnerability” (Grafana Labs, 2024).

Affected Grafana versions include:

- 9.5.0 to 9.5.17
- 10.0.0 to 10.0.12
- 10.1.0 to 10.1.8
- 10.2.0 to 10.2.5
- 10.3.0 to 10.3.4

(Grafana Labs, 2024).

This explains that the issue was patched, meaning that any version that was from 10.4.0 and above would not be impacted. Once again, it reiterates how bad an exploit can be as it can disrupt the environment, which can lead to real world impacts such as a user losing valuable time that can equate to loss of money. Now when creating a platform that users don't trust it can be due to the security measure not providing what was hoped for. Highlighting something as simple as overlooking a permission check can lead to vulnerability with endless scenarios that can be catastrophic.

Cybersecurity Event: CircleCI

Incident Summary

Aside from understanding and trying to interpret how an attacker can hack in the scenario of Grafana Labs, cybersecurity breaches and events can occur every day, showing how these events can cause fear within the developer community. In a recent incident that occurred a few years ago, attackers have been targeting supply chain software security. Stating that, "In January 2023, CircleCI disclosed that a cybercriminal had used malware on a CircleCI engineer's laptop to steal a valid, two-factor authentication (2FA)-backed single sign-on session, allowing the attacker to execute session cookie theft and impersonate the employee, gaining access to a subset of production systems" (Fourne, 2022).

Security Implications

This explains how the attack consisted of the attacker gaining access to a valid session token, which allows them to impersonate a legitimate user with access to all the information. This event is critical due to many companies using CircleCI to build, test, and deploy their applications, which could potentially expose sensitive data. This leads to fear from developers; now they must be sharper and more consistent when looking at their code to search for any vulnerabilities. Then again, this causes users not to trust a platform they might rely heavily on. This leads to a loss of business, as many users would feel that these breaches could happen again.

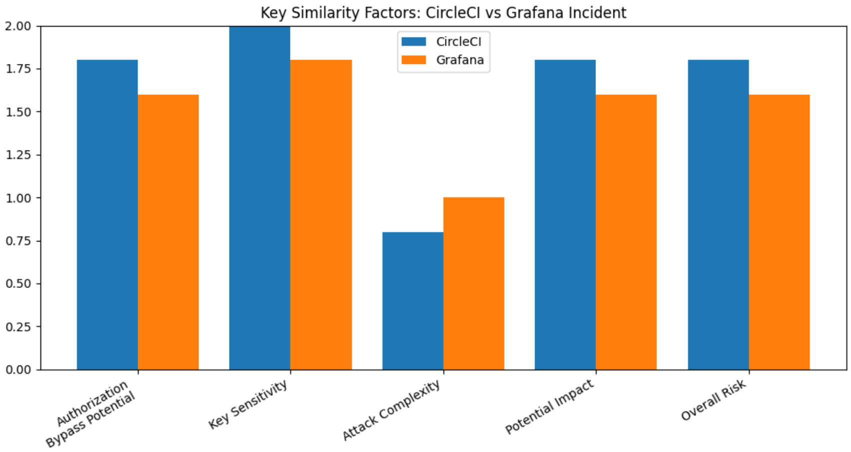
Developer Response

Apart from not trusting them when a security breach happens, it can be hard to answer all the customer questions. For example, the CircleCI incident report has stated, "Because this incident involved the exfiltration of keys and tokens for third-party systems, there is no way for us to know if your secrets were used for unauthorized access to those third-party systems. We have provided some details below to aid customers in their investigations." (Zuber, 2023). Therefore, this shows that even after recovery from an incident it is hard to know the extent of the organization's secret being exposed. This has led developers to implement a new security measure, whether that be tying these tokens with IP addresses, making these tokens short-lived, or implementing some behavioral analytics. This incident causes operational and data privacy risks, leading to potential financial loss. The implications of this event highlight the importance of policies because principles such as Least Privilege and Key Management need to be applied. Meaning that the token has to be made invalid as soon as it recognizes abnormal activity. This highlights the importance of good security and how it is essential to invest in security. This can be done by hiring more people or investing more money to be deemed secure.

Interconnection

The correlation between the CircleCI event and Grafana Lab CVE is how they both revolve around the Authorization Bypass Through User-Controlled Key. In the Grafana case, anyone with a valid snapshot key could bypass the authorization check, allowing them to delete the snapshot regardless of their role. Similarly, the attackers who exploited CircleCI only needed to gain access to the tokens from an internal user. Once in their possession, they were able to do as they pleased in the environment. Both of these events had a considerable amount of risk associated, and their issue stems from possessing a particular "key," whether found in the URL or the tokens. Overall, they display similar factors of having access to critical data components that they should not have.

Fig 2



Overview

The combination of threat intelligence, CVE analysis, and real-world cybersecurity events shows the necessity of strong security measures as our modern society continues to evolve. In Grafana's case, it enabled unauthorized users with valid snapshot keys to delete data, while in the CircleCI incident, it allowed attackers to impersonate employees through stolen tokens, ultimately gaining access to the production system. Both of these cases show how key implementation should not create system vulnerabilities, causing these organizations to start implementing processes, policies, and updates to code in order to be safe and secure. These cases show that modern cybersecurity strategies must evolve to protect against attackers whose goal is to disrupt even through the smallest oversight of mechanisms.

Recommendations

To prevent any from any similar vulnerabilities the following is recommended:

- Update to the newest version of Grafana
- Implement strict measures for access control
- Limit permission based on the least privilege principle
- Regularly audit and patch management system

References

CVE-2024-1313 grafana vulnerability in Netapp Products: Netapp product security. CVE-2024-1313 Grafana Vulnerability in NetApp Products | NetApp Product Security. (2024, March 24). https://security.netapp.com/advisory/ntap-20240524-0008/

Fourne, M., Wermke, D., Fahl, S., & Acar, Y. (2023, November 13). *A viewpoint on human factors in Software Supply Chain Security: A research agenda | IEEE Journals &*

Magazine | IEEE Xplore. A Viewpoint on Human Factors in Software Supply Chain Security. https://ieeexplore.ieee.org/document/10315781/

Mazon, R., & Chen, J. (2024, March 26). *Users outside an organization can delete a snapshot with its key*. cve.org. https://www.cve.org/CVERecord?id=CVE-2024-1313

Users outside an organization can delete a snapshot with its key. Grafana Labs. (2024, March 26). https://grafana.com/security/security-advisories/cve-2024-1313/

Zuber, R. (2023, January 13). *Circleci Incident Report for January 4, 2023 security incident*. CircleCI. https://circleci.com/blog/jan-4-2023-incident-report/