Oxeye Security Research Team Uncovers Vulnerability in Spotify's Backstage with CVSS Score of 9.8/10

New Vulnerability Discovered in Spotify's Backstage, a CNCF Incubated Project

TEL AVIV, ISRAEL, November 15, 2022 /EINPresswire.com/ -- Oxeye, the provider of award-winning cloud-native application security, today announced the presence of a critical new vulnerability in Spotify's Backstage project, calling on developers to take immediate action in their environments. By exploiting a VM sandbox escape through the third-party library in vm2, the Oxeye research team has gained the ability to conduct unauthenticated remote code execution in the Backstage project. Oxeye reported it through Spotify's bug bounty program, and Spotify rapidly patched the vulnerability and released Backstage version 1.5.1, which fixes the issue. Oxeye has published a detailed blog on the vulnerability.

Backstage unifies all infrastructure tooling, services, and documentation to create a streamlined development environment. Having more than 19,000 stars on Github, it is one of the most popular open-source platforms for building developer portals and is in widespread use by Spotify, American Airlines, Netflix, Splunk, Fidelity Investments, Epic Games, Palo Alto Networks and many others. Backstage was accepted to the Cloud Native Computing Foundation (CNCF) on September 8, 2020 and is at the Incubating project maturity level.

"By exploiting a vm2 sandbox escape in the Scaffolder core plugin, which is used by default, unauthenticated threat actors have the ability to execute arbitrary system commands on a Backstage application," said Yuval Ostrovsky, Software Architect for Oxeye. "Critical cloud-native application vulnerabilities like this one are becoming more pervasive and it is critical these issues are addressed without delay."

"Every research project we spin up starts with mapping potential inputs to an application. What caught our attention in this case were Backstage software templates and the potential for template-based attacks," said Daniel Abeles, Head of Research at Oxeye. "In reviewing how to confine this risk, we noticed that the templating engine could be manipulated to run shell

commands by using user-controlled templates with Nunjucks outside of an isolated environment."

Evaluating user-provided strings in a template engine can be dangerous since it exposes the application to such template-based attacks. The severity of an attack depends on the features the templating engine offers. In this case, the root of a template-based VM escape was able to gain JavaScript execution rights within the template. However, by using "logic-less" template engines such as Mustache, the introduction of server-side template injection vulnerabilities can be avoided. Separating the logic from the presentation as much as possible can greatly reduce exposure to the most dangerous template-based attacks.

"If using a template engine in an application, make sure to choose the right one in relation to security. Robust template engines are extremely useful but might pose a risk to the organization," said Gal Goldshtein, Senior Security Researcher at Oxeye. "If using Backstage, we strongly recommend updating it to the latest version to defend against this vulnerability as soon as possible."

Oxeye's DevSecOps and AppSec solution is designed for cloud-native application security testing and risk analysis and is enriched with infrastructure layer configuration data. The Oxeye security research team leverages the context-based and multi-dimensional vulnerability analysis capabilities built into the platform to help clear the noise of false positives caused by legacy solutions, and prevent false negatives. This ensures that security teams can focus their resources on other concerns putting the organization at risk.

If interested in learning more about how Oxeye can assist with cloud-native application security challenges, please visit https://www.oxeye.io/contact to contact us.

Resources:
- Take a deeper dive into the vulnerability by reading the blog entry on Oxeye's website at: https://www.oxeye.io/blog
- Follow Oxeye on Twitter at @OxeyeSecurity
- Follow Oxeye on LinkedIn at https://www.linkedin.com/company/oxeyeio/
- Visit Oxeye online at http://www.oxeye.io

About Oxeye
Oxeye provides a cloud-native application security solution designed specifically for modern container and Kubernetes-based architectures. The company enables customers to quickly identify and resolve all application-layer risks as an integral part of the software development lifecycle by offering a seamless, comprehensive, and effective solution that ensures touchless assessment, focus on the exploitable risks, and actionable remediation guidance. Built for Dev and AppSec teams, Oxeye helps to shift security to the left while accelerating development cycles, reducing friction, and eliminating risks. To learn more, please visit www.oxeye.io.

- END -

Joe Austin
Media
+1 818-332-6166
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
