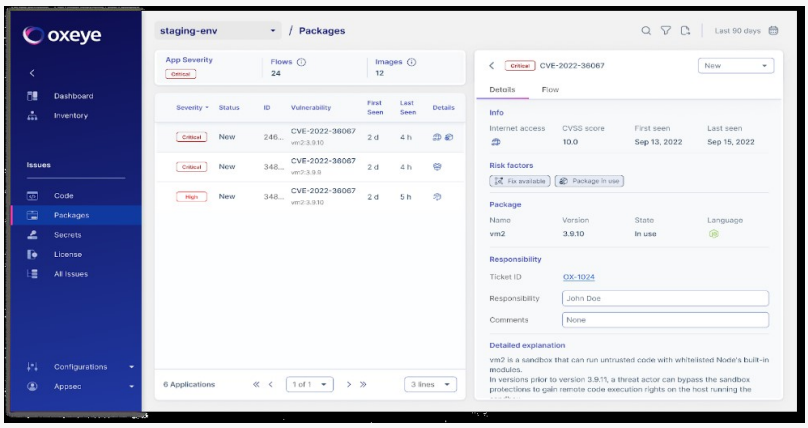
Oxeye Warns of “SandBreak” vm2 Vulnerability with CVSS Score of 10.0

At 16 Million vm2 Downloads Every Month, Potential Impact of SandBreak Widespread and Critical

TEL AVIV, ISRAEL, October 11, 2022 /EINPresswire.com/ -- Oxeye, the provider of award-winning cloud-native application security, today announced the discovery of a serious vm2 vulnerability that has received the maximum CVSS score of 10.0 with the following CVE (CVE-2022-36067). Called SandBreak and detailed on the Oxeye blog, this new vulnerability requires R&D leaders, AppSec engineers and security professionals to ensure they immediately patch the vm2 sandbox if they use it in their applications.

Oxeye Logo



vm2 is an extremely popular Javascript sandbox library, with 16 million downloads a month. It provides a commonly used software testing framework capable of running untrusted code synchronously in a single process. It is one of the more popular testing environments, in use by millions of developers because it allows full control over the sandbox’s console output with the ability to limit access to select built-in modules or securely call methods and exchange data between sandboxes.

The Oxeye research team found a critical sandbox escape vulnerability that leads to remote code execution in vm2. The vulnerability was disclosed to the project owners and was rapidly patched in version 3.9.11. GitHub issued advisory CVE-2022-36067 for this vulnerability and gave it a CVSS score of 10, putting AppSec professionals, developers, and others on alert.

A threat actor who exploits this vulnerability will be able to bypass the vm2 sandbox environment and run shell commands on the machine hosting it. Sandboxes serve different purposes in modern applications, such as examining attached files in email servers, providing an

additional security layer in web browsers, or isolating actively running applications in certain operating systems. Given the nature of the use cases for sandboxes, it's clear that the vm2 vulnerability can have dire consequences for applications that use vm2 without patching. The fact that this vulnerability has the maximum CVSS score of 10.0 and is extremely popular means its potential impact is widespread and critical.

According to Gal Goldshtein, Senior Security Researcher at Oxeye, "Our usual approach when evaluating a given software's security is first to analyze the previous security lapses discovered in the same software. This helps us better grasp the available attack surface and may also lead to low-hanging bugs stemming from incomplete fixes. It also helps us come up with techniques to bypass the implemented fixes. While reviewing the previous bugs disclosed to the vm2 maintainers, we noticed an interesting technique: the bug reporter abused the error mechanism in Node.js to escape the sandbox."

Yuval Ostrovsky, Architect at Oxeye added that "Although sandboxes are meant to run untrusted code within your application, you shouldn't automatically assume that they are safe. If the use of a sandbox is unavoidable, it is recommended to separate the logical sensitive part of your application from the microservice that runs the sandbox code so if a threat actor successfully breaks out from the sandbox, the attack surface is limited to the isolated microservice."

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 that help clear the noise of false negatives and false positives caused by legacy solutions to make sure security teams are focused on the most critical risks.

"We make vulnerability insights smarter by differentiating which dependencies in the application are merely installed and which are actually loaded and used by the application," said Daniel Abeles, Head of Research at Oxeye. "This allows us to rank the severity of vulnerable packages, such as the vm2 package, within the application in order to help focus on remediation efforts that address the most important vulnerabilities first. We are helping to cancel noise in application security."

If interested in learning more about how Oxeye can assist with cloud-native application security challenges, please visit https://www.oxeye.io/get-a-demo to register for a demonstration.

Resources:
- Take a deeper dive into the vulnerability by reading the blog entry on Oxeye's website - www.oxeye.io/blog/vm2-sandbreak-vulnerability-cve-2022-36067
- 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 -

Dean Agron
Oxeye
+972 54-672-2465
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
