Oxeye AppSec Platform Automatically Identifies Zero-Day Vulnerability in HashiCorp Vault Project

Newly Discovered Issue Presents Risk – Immediate Patching is Key to Maintaining the Integrity and Confidentiality of Sensitive Information

TEL AVIV, ISRAEL, April 12, 2023 /EINPresswire.com/ -- Oxeye, the provider of an award-winning cloud-native application security platform, today announced the discovery of a new vulnerability in the HashiCorp Vault Project that has now been patched. HashiCorp Vault is a popular identity-based secrets and encryption management system used to control access to API encryption keys, passwords, and certificates. The vulnerability was automatically discovered and reported by the Oxeye Platform during a deployment, with no manual input or intervention, and was revealed to be an SQL injection vulnerability that potentially could lead to a Remote Code Execution (RCE). This vulnerability had been completely overlooked by other application security tools used at the time. Oxeye reported this vulnerability to HashiCorp and the team quickly patched it in versions 1.13.1, 1.12.5, and 1.11.9. of Vault. HashiCorp has issued CVE-2023-0620 for this vulnerability and updated the threat model in their documentation in response to this discovery.

HashiCorp Vault provides encryption services for modern, microservices-based applications which often require the use of a multitude of secrets. With Vault, these secrets are gated by authentication and authorization methods using HashiCorp's UI, CLI, or HTTP API. Access to secrets and other sensitive data can be securely stored and managed, tightly controlled (restricted), and is auditable.

The Oxeye Application Security Platform automatically identified this new vulnerability as part of a standard deployment scan and found that attackers could use this vulnerability to access sensitive data, modify or delete it, and run malicious code on the target system. Given the trend toward microservices in modern software development, configuration-based attacks like this are a significant threat and are expected to become more common. Because the centralized nature of configurations makes them a single point of truth, they are a lucrative target for threat actors. As such, organizations should prioritize the security of configuration files and other centralized

components in modern applications.

The vulnerability exists in how Vault handles SQL queries when interacting with its backend database. Attackers can exploit this vulnerability by injecting malicious SQL statements into the configuration parameters Vault loads at startup. If successful, the attacker can run arbitrary SQL queries on the target database. In some cases, depending on the database configuration, the threat actor can escalate the vulnerability to execute arbitrary system commands on the machine hosting the database.

Organizations that use HashiCorp's Vault in their infrastructure should prioritize patching their installations and review security policies to prevent similar vulnerabilities from being exploited in the future. The vulnerability affects Vault versions up to 1.13.0 and has been fixed in versions 1.13.1, 1.12.5, 1.11.9. More information can be found in this HashiCorp bulletin - shorturl.at/jtwER.

"The importance of restricting access to critical tools and implementing adequate input validation to prevent SQL injection attacks is highlighted by this vulnerability in HashiCorp's Vault project," said Ron Vider, CTO and Co-Founder for Oxeye. "To safeguard your environment, swiftly applying patches and ensuring security policies are current will ensure successful attacks are avoided."

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:
- 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
