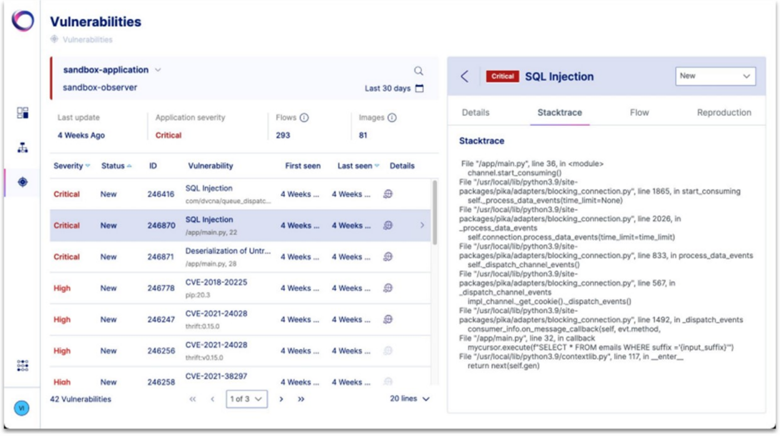
EINPRESSWIRE

Oxeye Announces General Availability of Cloud Native Application Security Testing Platform at KubeCon 2022

Company Contextualizes Cloud Native Application Risk Assessment -- Investigates Application-Level Vulnerabilities



Last update	Application severity	Flows	Images
4 Weeks Ago	Critical	293	81

Severity	Status	ID	Vulnerability	First seen	Last seen	Details
Critical	New	246416	SQL Injection com/dvcna/queue_dispatc...	4 Weeks ...	4 Weeks ...	
Critical	New	246870	SQL Injection /app/main.py, 22	4 Weeks ...	4 Weeks ...	
Critical	New	246871	Deserialization of Untr... /app/main.py, 28	4 Weeks ...	4 Weeks ...	
High	New	246778	CVE-2018-20225 pip:20.3	4 Weeks ...	4 Weeks ...	
High	New	246247	CVE-2021-24028 thrift:0.15.0	4 Weeks ...	4 Weeks ...	
High	New	246256	CVE-2021-24028 thrift:v0.15.0	4 Weeks ...	4 Weeks ...	
High	New	246258	CVE-2021-38297	4 Weeks ...	4 Weeks ...	

42 Vulnerabilities « ‹ 1 of 3 › » 20 lines

Critical SQL Injection New

Stacktrace

```
 File "/app/main.py", line 36, in <module>
   channel.start_consuming()
File "/usr/local/lib/python3.9/site-
packages/pika/adapters/blocking_connection.py", line 1865, in start_consuming
   self._process_data_events(time_limit=None)
File "/usr/local/lib/python3.9/site-
packages/pika/adapters/blocking_connection.py", line 2026, in
_process_data_events
   self.connection.process_data_events(time_limit=time_limit)
File "/usr/local/lib/python3.9/site-
packages/pika/adapters/blocking_connection.py", line 833, in process_data_events
   self._dispatch_channel_events()
File "/usr/local/lib/python3.9/site-
packages/pika/adapters/blocking_connection.py", line 567, in
_dispatch_channel_events
   impl_channel._get_cookie()._dispatch_events()
File "/usr/local/lib/python3.9/site-
packages/pika/adapters/blocking_connection.py", line 1492, in _dispatch_events
   consumer_info.on_message_callback(self, evt.method,
File "/app/main.py", line 32, in callback
   mycursor.execute(f"SELECT * FROM emails WHERE suffix ='{input_suffix}'")
File "/usr/local/lib/python3.9/contextlib.py", line 117, in __enter__
   return next(self.gen)
```

Oxeye Logo

TEL AVIV, ISRAEL, May 17, 2022 /EINPresswire.com/ -- Oxeye, provider of award-winning cloud-native application security testing platform, today announced the general availability of its Cloud Native Application Security Testing (CNAST) platform at KubeCon 2022 in Valencia, Spain. The advanced platform identifies custom code and open-source vulnerabilities, as well as software secrets to reveal the critical, exploitable security issues as an integral part the software development lifecycle. As a result, developers and application security teams receive clear insights that accelerate proper mitigation.

With a large number of organizations today hosting application workloads in the cloud, it is imperative that application security be implemented to accommodate the unique security requirements of cloud-based applications. Meeting this challenge head-on, the Oxeye Cloud Native Application Security Testing platform is built from the ground up with the same high degree of agility and scale of cloud infrastructure to address the pervasive number of vulnerabilities materializing in these environments.

Cloud native application security testing by Oxeye is focused on the cloud native segment of the AST market. This is imperative as AppSec and DevSecOps professionals are confronted with millions of cloud-native apps industry-wide. In order to protect this new application architecture, the next-generation application manager will be required to conduct proper infrastructure hygiene. To this end, Oxeye supports scalable, ever-changing environments and automatically adapts to changes for an agile testing scope without changes to code or the need to manually intervene.

“Oxeye’s approach allows us to embed context-aware, application security testing at the most critical point of our development cycle,” said Omer Azaria, VP, Engineering, Sysdig. “This leaves no stone unturned as the solution analyzes all potential applicative threats. Included is the deep mapping of all app components and how they communicate with each other; lightweight intelligent testing for active validation, and the context we need in order to map the findings back to teams and dev owners.”

Key capabilities include:

- Cloud Native Application software bill of materials (SBOM) - Through Oxeye’s unique integration into each application, the platform provides users with an elaborate software bill of materials, deep from within cloud-native environments.

- Cloud Native Application Security Testing Built for Modern Architectures – Oxeye analyzes application code across microservices to identify code vulnerabilities, vulnerable 3rd party packages, and hardcoded secrets as part of the software development lifecycle for clear guidance that enables accurate remediation.

- Multi-Layer and Multi-Service Identification of Exploitable Vulnerabilities -
Provides Runtime Code Analysis with no code changes, Vulnerable Flow Analysis to detect vulnerabilities across application microservices, and Active Validation with automatic creation and execution of security tests to validate vulnerabilities prior to reporting.

- Contextual Risk Assessment - Enriches data with infrastructure configuration information from the container, cluster, and cloud layers to calculate risks based on Internet accessibility, sensitive data processing, flawed configuration, etc.

- Clear Remediation Guidance for Developers – Provides developers with application analysis in runtime to reproduce each step of vulnerability exploitation, delivery of the exact line of code where the vulnerability is executed, and vulnerability flow visibility for accurate execution flow tracing that allows for fast identification and remediation of actual issues.

“Modern applications introduce major challenges to Application Security leaders, with prioritization, visibility, and collaboration on top,” said Dean Agron, Co-Founder, and CEO of Oxeye. “The Oxeye platform is the best option for modern application security testing as its vulnerability detection accuracy is second to none. The powerful solution greatly reduces security risk throughout every stage of software development and deployment, alongside providing clear visibility into the application structure and building blocks”

To meet with Oxeye at KubeCon 2022 and learn more about the company’s Cloud Native

Application Security Platform, visit booth #SU34 during the event.

Pricing and Availability
Oxeye Cloud Native AST is generally available as of this release. The company invites developers, DevSecOps and other interested parties to learn more by visiting https://www.oxeye.io/solution.

Or, please schedule a personalized demo at https://www.oxeye.io/get-a-demo.

Resources:

- Follow Oxeye on Twitter at @OxeyeSecurity
- Join 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 testing solution designed specifically for modern architectures. The company enables customers to identify and resolve the most critical code vulnerabilities as an integral part of the software development lifecycle, disrupting traditional application security testing (AST) approaches by offering a contextual, effortless, and comprehensive solution that ensures no vulnerable code ever reaches production. 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
Public Relations
+1 818-332-6166
email us here
Visit us on social media:
Twitter
LinkedIn