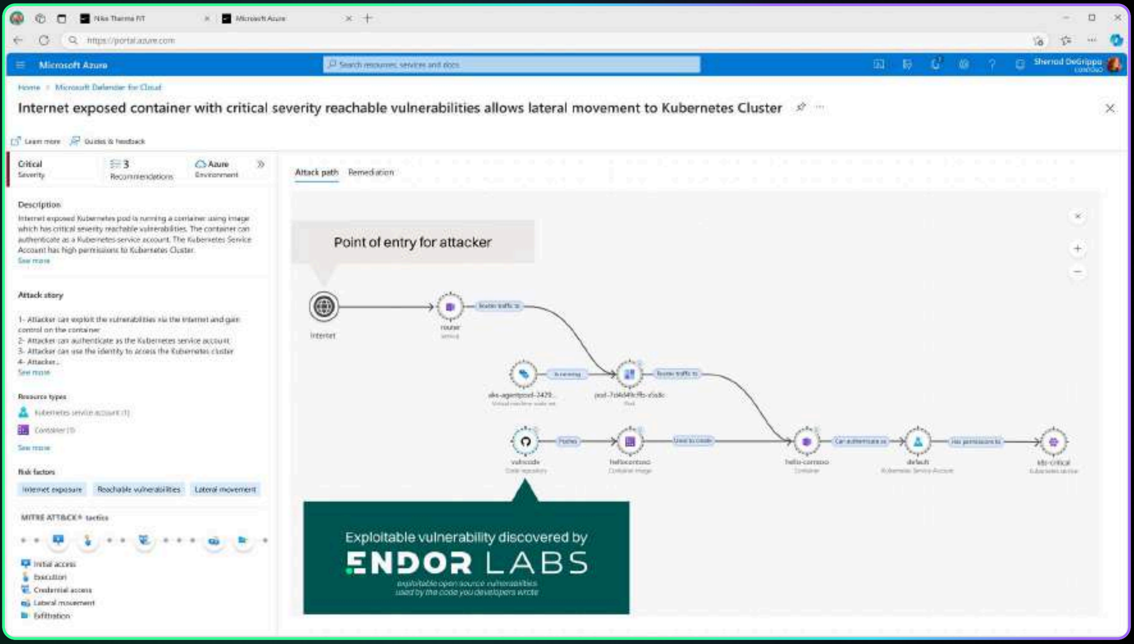
ENDOR LABS

Secure AI-Assisted Development from Code to Cloud

As AI accelerates how software is built, traditional AppSec tools are falling behind. Endor Labs and Microsoft are redefining what modern application security looks like by combining deep code intelligence with Microsoft's cloud-scale protection to secure applications from the first line of code to runtime in the cloud



Internet exposed container with critical severity reachable vulnerabilities allows lateral movement to Kubernetes Cluster

Description

Internet exposed Kubernetes pod is running a container using image which has critical severity reachable vulnerabilities. The container can authenticate as a Kubernetes-service account. The Kubernetes Service Account has high permissions to Kubernetes Cluster.
See more

Attack story

1- Attacker can exploit the vulnerabilities via the Internet and gain control on the container
2- Attacker can authenticate as the Kubernetes service account
3- Attacker can use the identity to access the Kubernetes cluster
4- Attacker...
See more

Resource types

Kubernetes service account (1)
Container (1)
See more

Risk factors

Internet exposure | Reachable vulnerabilities | Lateral movement

MITRE ATT&CK® tactics

- Initial access
- Execution
- Credential access
- Lateral movement
- Exfiltration

Built for the AI Era

AI is changing how code gets written, and what needs to be secured

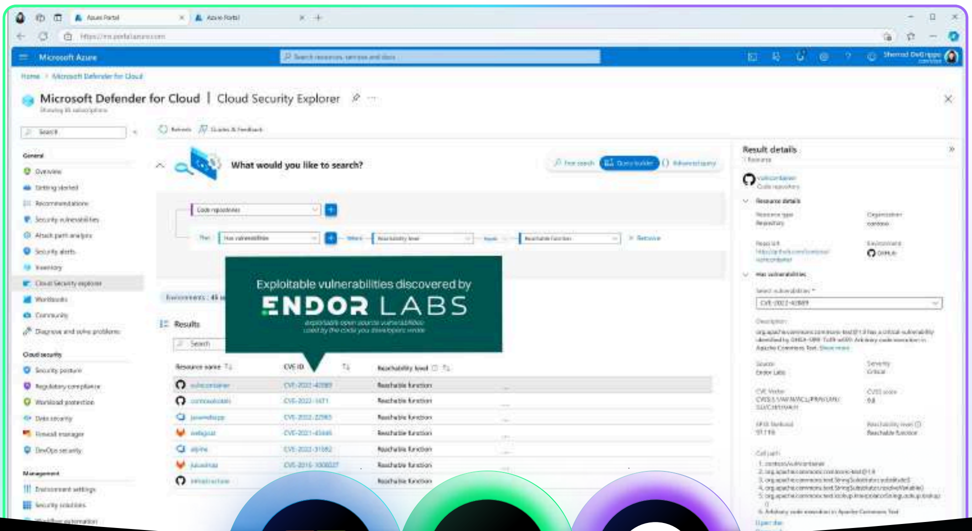
Endor Labs is the AppSec platform built to secure how modern software is built, fast, open source-driven, and increasingly AI-generated. We build a complete graph of your software estate, so teams can pinpoint and fix critical risks in complex, dependency-rich code, whether written by humans or AI.

Together with Microsoft, we bring this intelligence to GitHub, Azure DevOps, and Defender for Cloud.

From Code Risk to Runtime Exploitability

Endor Labs + Microsoft Defender for Cloud

- Map cloud attack paths with Microsoft Defender.
- Enrich attack patch with Endor Labs' reachability analysis to show which vulnerabilities can actually be exploited.
- **Result:** Security teams know what's exploitable and what to fix first.



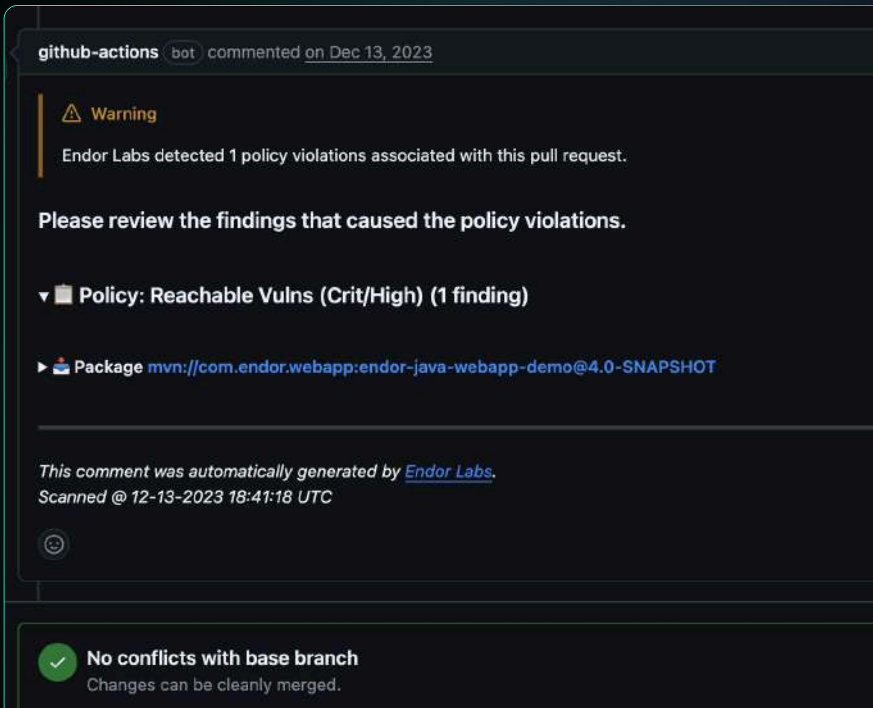
Exploitable vulnerabilities discovered by ENDOR LABS

Resource name	CVE ID	Reachability level
vulncontainer	CVE-2022-42889	Reachable function
contosoaksbb	CVE-2022-1471	Reachable function
javawebapp	CVE-2022-22965	Reachable function
webgoat	CVE-2021-45046	Reachable function
alpine	CVE-2022-31692	Reachable function
juiceshop	CVE-2016-1000027	Reachable function
infrastructure	[illegible]	Reachable function

Developer-Centric AppSec in GitHub

Endor Labs + GitHub Advanced Security

- Slash SCA noise by 92% with function-level reachability
- Fix CVEs 6.2x faster with contextual remediation
- Use a backported security patches to fix EoL software or hard-to-fix upgrades
- Encourage CoPilot adoption by securing AI-generated code



github-actions bot commented on Dec 13, 2023

> ⚠ Warning
>
> Endor Labs detected 1 policy violations associated with this pull request.

Please review the findings that caused the policy violations.

▾ 📋 **Policy: Reachable Vulns (Crit/High) (1 finding)**

▸ 📦 **Package** mvn://com.endor.webapp:endor-java-webapp-demo@4.0-SNAPSHOT

This comment was automatically generated by Endor Labs.
Scanned @ 12-13-2023 18:41:18 UTC

✓ **No conflicts with base branch**
Changes can be cleanly merged.

Go-to-Market Ready

MACC Eligible:

Accelerate Azure consumption with secure-by-default development

Azure Marketplace:

Available now for easy procurement

IP Co-Sell Ready:

Fully aligned with Microsoft sales motions

For more information on co-selling opportunities and solutions, contact our partnerships team:

escherr@endorlabs.ai

www.endorlabs.com

Additional Resources:

GitHub Advanced Security Integration

→ https://github.blog/security/from-finding-to-fixing-github-advanced-security-integrates-endor-labs-sca/
→ https://www.endorlabs.com/learn/endor-labs-github-advanced-security

Microsoft Defender for Cloud Integration

→ https://www.endorlabs.com/learn/microsoft-defender-for-cloud-natively-integrates-with-endor-labs
→ (https://techcommunity.microsoft.com/blog/microsoftdefendercloudblog/bringing-appsec-and-cloudsec-together-microsoft-defender-for-cloud-integrates-wi/4372366

Azure DevOps Integration

→ https://docs.endorlabs.com/deployment/monitoring-scans/azure-app/
→https://docs.endorlabs.com/deployment/ci-scans/scan-with-azuredevops/

AppSec for the Software Development Revolution

Ready to
Book a Demo?

endorlabs.com/demo-request