The new OWASP Top Ten helps CISO’s make better decisions

Focusing on known, high risk bugs in Vulnerable & Outdated Components means a more secure enterprise, but new tools are needed to realize the benefit

In the last in our Q & A series on the 2021 OWASP Top Ten list of web application risks, Waratek Founder & CTO John Matthew Holt discusses what it will take to realize for CISOs to realize the benefits of a more focused and scalable security program. The following is an edited version of John Matthew’s comments. Listen to the full commentary (5:14).

Q: What does the new OWASP Top Ten list mean for CISO’s who are looking for ways to prioritize their team’s efforts?

JMH: A CSO doing risk assessment across their many applications, systems, technologies, platforms, et cetera, at the end of the day, what matters to him or her is not how many vulnerabilities of a given type do I have. He wants to know that, but that's secondary to what is readily exploitable now today. What can take my business down in five minutes because it's vulnerable now? If you have anything (other vulnerability), that needs to be tracked. There needs to be remediative efforts made. But, those other things are not going to bring your business down in 60 seconds flat, like a highly exploitable, known vulnerability with a high impact.

Q: OWASP now recognizes the increasing risk from legacy apps and components. What needs to happen to improve the security posture of enterprises with vulnerable & outdated components?

JMH: There's an opening there, and there's a gap in the tool chain for addressing these difficult scenarios where you can't change your component because it breaks your app. That's where a new set of tools a) is needed and, b) where we're seeing a new set of tools kind of come into existence and fill that void. They move the security and analytics, and they move the security, action, and control from being at the development time to the production time running inside the application stack.

These tools introduce some trusted, small pieces of autonomous code whose job it is to study the application as it's executing. They watch the applications in much the same way that APM performance monitoring tools like App Dynamics and New Relic watch your code and watch your memory for performance purposes, but instead look at the security posture and, among other things, the use of vulnerable to outdated components in your applications. Then you go through different ways and different means using those agents to apply mitigations or remediations to these outdated components proactively or reactively.

Now is the first time that these problematic, vulnerable, and outdated components can be (easily) addressed and can be addressed at scale.

Q: You’ve said that automation is the answer to the issue of security at scale. Why?

JMH: That is the only way Waratek or anybody else is going to be able to solve security at scale. If it needs human beings to kind of, you know, tweak knobs and tweak dials on a per application basis, then you're in the same kind of high cost, high effort loop of maintenance for things, like firewalls / web application firewalls as an example, back in development time. But, you can take that away and you can make your agents autonomous so that they become the Tesla of self-driving security where you set your destination. If you have little autonomous agents who can proactively hunt for these (vulnerabilities & outdated components) behind the scenes in real-time, and then go ahead and apply mitigation or remediation, in real-time, then suddenly you've got a tool that can not only address this security gremlin that's hiding in everyone's stacks, but you can do it at scale. Not just for one app or for two apps in your in your enterprise, but you can do it for 100 or 200 or a thousand apps for the same effort that it takes to do one, two, or three.

Q: If CISOs are better able to match effort to risk, is there a broader implication for application security in general?

JMH: Application security has kind of been the laggard, it's been a late bloomer compared to the other categories of security. I think this is part of a trend of application security generally as a category, getting more airtime and more of the recognition it needs because it's the front-line defense now for applications. If you break the app, you get the data, and the data is the most important thing in enterprises.

I think it's going to help drive maturation in the way security operators and practitioners contemplate cybersecurity risk for their enterprises and organizations and how they can plan around that.

Listen to John Matthew’s full comments on how the 2021 OWASP Top Ten helps CISO’s better manage risk (Time to Listen – 5:14)

Previous Q & A

What’s the big deal about the new OWASP Top Ten?

Listen to John Matthew’s full comments on the strategic shift in the 2021 OWASP Top Ten from incident rate-based to risk-based (Time to Listen - 3:33)

OWASP looks at the rising risk of vulnerable components

Listen to John Matthew’s full comments on the Vulnerable & Outdated Components category in the 2021 OWASP Top Ten (Time to Listen - 6:51)