OWASP looks at the rising risk of vulnerable components

What that means for your threat landscape, teams, and tools

This month and next, Waratek Founder & CTO John Matthew Holt discusses the changes in the 2021 OWASP Top Ten list of web application risks. This week's focus is on the move up the rankings from #9 to #6 of known vulnerabilities. The following is an edited version of John Matthew's comments. Listen to the full commentary (6:51).

Q: What is the most significant change in the 2021 OWASP Top 10 from the previous list?

In the 2017 list, there were two of the 10 categories related to injection. Why? Because if you're measuring by incidents, those are different types of vulnerabilities that have different counts. Makes sense, but it doesn't really help you on a strategic view. There's a different ratio of risk there, and that wasn't captured well in the 2017 rankings.

The change that has taken place in the OWASP rankings between '17 and '21 is to move to a mentality that's thinking about exploitability. If you only solve all of the highly exploitable, high-impact vulnerabilities and even don't address anything else, you immediately can sleep easier at night than the person who addresses, you know, the top three incidents' vulnerabilities with no regard to exploitability.

Q: You believe moving previous category #9 – Using Components with Known Vulnerabilities to the #6 - Vulnerable & Outdated Components position will have far reaching impacts. Why?

Vulnerable and outdated components is the category that captures, among other things, third-party components. What we have seen over the last 10-odd years is the ratio of business logic code to third-party components has been increasing in favor of third-party components. But, there's a big security gremlin hiding in that detail.

From an economies of scale perspective, malicious operators get bigger bang for their buck, no pun intended, by finding vulnerabilities in invulnerable and outdated software components that are part of application supply chains and with no business logic. So that's important. And I think I think what we're seeing with the rise of vulnerable, outdated components from number nine in 2017 to number six in 2021 is that thematic element coming through.

Q: What's stopping teams from fixing vulnerable components?

Whilst there are a range of developer tools that target vulnerable and outdated components, things like software composition analysis (SCA) tools as an example, they are all developer oriented. But, you can't just pluck one vulnerable, outdated component and drop a newer version of that component in an application, which has a 99 other components, with the expectation it will work seamlessly the next day.
(continued)

It doesn't work because that new version of the component, which fixes the vulnerability, has some other unintended changes which break compatibility. This is a real problem, and there's no tooling to deal with that side of the problem. When SCA works, it works well; but when it doesn't - and increasingly it doesn't - it's hard to make it work reliably at scale. Then, suddenly, people are tooless and to some degree, helpless because they're trapped on vulnerable, outdated components.

Q: How does changing the OWASP Top Ten List help address the issue of vulnerable components?

This is going to ripple down to developers to help them re-orient as they are learning about security. Both old developers, new developers learning about security will re-orient them to think about what's important in security. I think it helps security practitioners as well to sharpen their focus on what they really need to care about. Also even for vendors, for tech companies like Waratek, they should be focusing their efforts on the highly exploitable, high-impact vulnerabilities so that they can give the biggest bang for the buck to their customers in terms of addressing and removing risk.

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

December 2nd: The problem with updating legacy components & the 2021 OWASP Top Ten