Trusted CI Success Story
Open XDMoD

Trusted CI helps Open XDMoD harden its defenses

When software developers go to hacker conferences, it can be intimidating. Code exploitation methodology can make developers feel vilified for creating vulnerabilities. Yet, the goal of most hackers is not to make developers feel bad or point blame about code. Instead, hackers simply want to contribute to an adequate fix. At least that's the experience of Ryan Rathsam, scientific programmer for the XMS project team, which developed XDMoD and Open XDMoD.

"We try our best, but we are software developers and not cybersecurity experts. As software creators, we realize it is important to secure our product for the academic and high-performance computing (HPC) sphere," said Rathsam.

Open XDMoD is an open source analytics platform that collects utilization performance and quality service data for the National Science Foundation's (NSF) extreme digital resources and network. "Our goal is to improve operational efficiency and management," explained Rathsam. "Open XDMoD provides a web portal for graphical analysis of HPC environments, and XDMoD users make decisions based on our information."

"Cybersecurity has always been present in the development of XDMoD, but we wanted to ensure that our software users could trust that they would not be opening themselves up to a large amount of risk. We wanted to make it as hard as possible for malicious actors to compromise our system, thus using XDMoD as a pivot to get further into a user's network," said Rathsam.

"We knew we didn't have the cybersecurity expertise in house, and that led us to Trusted CI. After submitting an application for a 2020 engagement slot, we were very thankful to be chosen," added Rathsam.

As part of the engagement, Trusted CI, the NSF Cybersecurity Center of Excellence, examined ways to harden Open XDMoD against various threats, scrutinizing the software's coding practices and identifying vulnerabilities. Furthermore, Trusted CI recommended the development of vulnerability disclosure and remediation policies that were accessible to the public. "The policies assure external security researchers that we will remediate vulnerabilities that are reported to us, and it lets them know how we will communicate with them. It's helpful to have policies and procedures in place ahead of any issues that might arrive," emphasized Rathsam.

Another overarching theme of the engagement was not only making the software configuration safe by default but also making it extremely difficult for users to override security measures, explained Rathsam.

Open XDMoD provides analytics for NSF-funded academic and high-performance computing (HPC) researchers.

"None of us at XDMoD had engaged with an external entity before. Trusted CI was good at walking us through the process, how it would work, what to expect, here's what we're doing. It was a very smooth and easy process working with them. We enjoyed it," said Rathsam.

Open XDMoD implemented all of the Trusted CI recommendations. "With all of these updates and, more importantly, the mindset this engagement has engendered in the team, we will be more mindful of security while developing new features," added Rathsam. "Our overall quality and security will continue to improve, which means that users will feel more safe and secure in installing and utilizing XDMoD. And that leads to increased adoption."