Testimony of Chris Wysopal, CTO & co-founder of Veracode

Co-chairs and members of the committee, thank you for inviting me to testify today about application security, which concerns reducing the vulnerabilities that pervade custom, commercial, and open source software and are one of the most prevalent causes of data breaches. This is a great honor for me. The company I founded 17 years ago, Veracode, is currently helping secure the software of more than 2600 organizations, including large city governments, several state governments and U.S. federal agencies such as the IRS and SEC. Before founding Veracode I was a vulnerability researcher whose research into critical vulnerabilities led to me testifying for the U.S. Senate's first hearing on government computer security in 1998.

Today I would like to cover how software vulnerabilities and supply chain risks are leading to breaches of many organizations and how this risk can be managed with the application security testing of code as it is developed. The developers of software are in the best position to keep users of the software and their data secure. We don't rely on automobile drivers alone to have safe highways. Cars are designed and tested for safety. The same is true for software. Unless security is designed in and tested for during the software development process, we fight a losing battle keeping users and data secure. We need software that is "secure by design."

In March 2022, the incident response company, Mandiant, published details they uncovered investigating attacks on 6 state governments[1]. The Chinese cyberthreat group, APT41, was to blame. There were 3 different types of attacks against web sites run by those states that I would like to explain.

The first type is known as a supply chain attack. Organizations running the vendor supplied Acclaim USAHERDS software, which is used by states for animal health management, were compromised by a vulnerability in the web application. In a supply chain attack the attackers first insert malicious code in the software by compromising the vendor, which we saw this in the much-publicized Solar Winds attacks, or they discover a vulnerability in commercial software and then attack the users of the software. In this case it was the latter. The vendor could have prevented this attack if they had performed automated application security testing and other security reviews as part of their software development process.

When software is acquired from a vendor there needs to be scrutiny by the customer of what security processes were used in the development of that software. Organizations can then reject software built without a "secure by design" process. Software supply chain security is one of the major actions the U.S. Federal Government is taking to secure itself, which is described in the 2021 Executive order "Improving the Nation's Cybersecurity"[2].

The second type of attack, that compromised the 6 states, was APT41 discovered and exploited vulnerabilities in the custom web apps built by state employees or contractors. Custom web apps require application security testing be performed during the development process as programming code is written and built. Unless security testing is performed, the result will be an application that contains vulnerabilities. When Veracode surveyed all the 750,000 applications built by its 2600 customers over the last 12 months, it found that 80% of applications contained vulnerabilities and 20% contained high severity vulnerabilities[3]. This is the current industry norm.

The third type of attack by APT41 is a combination of the first two, as it concerns both the software supply chain and custom app development. This attack exploits known vulnerabilities in the open-source components that are used during custom web app development. Much like a modern car is assembled from parts from many suppliers, modern software is constructed with freely available, open-source components. Like we have seen with safety defects in air bags and tires for auto parts, open-source components can have defects which lead to vulnerabilities. When those components are used during development the application will often inherit a vulnerability from the component. The team building the app is responsible for making sure it is secure, so they need to scan the application for vulnerable components and remediate them. The popular and vulnerable open-source component named Log4j was used to build custom web apps at some of the 6 states. This allowed APT41 to launch successful cyberattacks. When the vulnerability in Log4j was made public in Dec 2021, Jen Easterly, the Director of the DHS Cybersecurity and Infrastructure Security Agency said of the vulnerability, "this is one of the most serious I've seen in my entire career, if not the most serious."

The three types of successful cyberattacks on the web sites of 6 states could have been made far less likely if each type of attack was prevented during software development. It might be tempting to think if only the states had used more sophisticated endpoint or network protection this wouldn't have happened. But just like you need to add crumple zones and airbags to a car during its design and construction, you need to build security into software. We need software to be "secure by design."

When software is developed, automated application security testing should be performed to detect vulnerabilities in the code so that the programmers can remediate them. Open-source scanning should also be performed to determine what vulnerable open-source components are used so they can be updated to new versions without those vulnerabilities. Finally, if software is acquired from a vendor, transparency should be required during the acquisition process to determine if the vendor performed these security processes. Giving software developers education around secure coding and access to application security testing tools is necessary to protect the data that is accessed through the web applications that Oregon government organizations build and use.

1. "Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments", Mandiant, 3/8/2022, https://www.mandiant.com/resources/blog/apt41-us-state-governments
2. Executive Order 14028, "Improving the Nation's Cyber Security", Executive Office of the President, 5/12/202,1https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
3. "State of Software Security 2023", Veracode, 1/11/2023, https://www.veracode.com/state-of-software-security-report