02.05.2024 – 14:05 Uhr

Horizon3.ai Unveils Rapid Response Service for Cyber Resilience

Horizon3.ai Unveils Rapid Response Service for Cyber Resilience

Empowering Organizations to Preemptively Address and Prioritize Confirmed Exploitable Vulnerabilities

SAN FRANCISCO, May 2, 2024 – Horizon3.ai, a pioneer in autonomous security solutions, today announced the launch of its **Rapid Response** service, now part of the NodeZero™ platform. This one-of-a-kind capability marks a significant advancement in autonomous penetration testing solutions by addressing a critical gap in measuring the real-world impact of exploitable vulnerabilities within the software many organizations have come to rely on. Now, organizations can gain a clear understanding of their 'likelihood of exploitability' for the most critical vulnerabilities being announced.

As organizations continue to contend with both zero-day and N-day vulnerabilities, the window of time between the public disclosure of a vulnerability and threat actors exploiting them in the wild is steadily shrinking. Knowing this predicament, organizations spend vast amounts of time, money, and resources patching the software they use after hearing of a vendor vulnerability announcement. Yet, how often are organizations expending considerable effort not knowing if a vulnerability is actually exploitable or not? The answer to that is, "quite often."

So far in 2024, the US National Vulnerability Database (NVD) has tracked 12,384 new vulnerabilities in publicly-released software. A common challenge for organizations is determining whether software they are using, identified as vulnerable, is actually exploitable within their specific environments, a judgment often contingent on how the software is deployed. Since organizations often lack a proven method to assess the 'exploitability' of software, they may find themselves updating software that does not require immediate patching. NodeZero addresses this issue with its Rapid Response service, which is specifically tailored to manage many of the most critical vulnerabilities more effectively. The following outlines the workings of the Rapid Response service.

As Horizon3.ai's attack team conducts original research and uncovers new vulnerabilities, they also keep an eye on public vulnerability disclosures. They assess the exploitability of these vulnerabilities, considering factors such as the ease of exploitation, their severity, and the prevalence of the vulnerable software. Following their assessment, they develop proof of concept (POC) exploits, integrate them into NodeZero as new attack content, and notify customers about these emerging vulnerabilities. With NodeZero, customers can probe their systems using this new attack content to gain immediate insights into their level of exploitability. Furthermore, Horizon3.ai alerts customers if known vulnerable software is present in their production environments and warns them about NodeZero being able exploit these weaknesses.

The Rapid Response service doesn't just focus on vulnerabilities; it zeroes in on the exploitability of known issues in production environments. As part of this service, organizations receive proactive measures to keep abreast of cyber-attacks. The vulnerabilities that flow through this program typically revolve around publicly accessible assets since they are the most likely targets for exploitation.

Recognizing the critical role of response time to emerging exploits in the wild, Horizon3.ai's Rapid Response service is designed to provide organizations with a proactive defense mechanism to stay ahead of evolving cyber-attacks as they're discovered or trending in the wild. The fundamentals of this type of rapid response effort are concentrated on enabling organizations to preemptively mitigate nascent vulnerabilities before threat actors target them.

"In the swiftly evolving arena of cybersecurity, where threats emerge and proliferate with alarming speed, the essence of a robust defensive posture lies in responding rapidly. We enable organizations to move faster by prioritizing critical vulnerabilities that have the most potential impact on their organization," says Snehal Antani, CEO and Co-founder of Horizon3.ai. "Our Rapid Response service is engineered to provide a preemptive shield, arming cybersecurity teams with the necessary knowledge, insights, and tools they need to protect their vital infrastructure."

By leveraging Horizon3.ai's expertise in using 'offense to inform defense', and leaning into NodeZero's autonomous capabilities, customers can schedule and/or immediately launch NodeZero using a single exploit-check to gain early detection of exploitability from an attacker's perspective. Once finished, NodeZero prioritizes the most critical and exploitable vulnerabilities that must be patched because they have been deemed as being completely exploitable by the NodeZero platform.

Horizon3.ai's Rapid Response service is a groundbreaking step forward in the field of cybersecurity, offering organizations an unprecedented level of preparedness against cyber threats. With its cutting-edge technology and proactive strategy, Horizon3.ai is redefining the landscape of cyber defense, providing a critical service that ensures organizations are not only aware of their vulnerabilities but are also equipped to address exploitability with unmatched speed and efficiency. This service, seamlessly integrated into the NodeZero platform, solidifies Horizon3.ai's position as a leader in autonomous security solutions, empowering organizations to fortify their defenses against the unpredictable nature of cyber threats.

Learn more about the Horizon3.ai Rapid Response service.

For more information, send your inquiry to info@horizon3.ai.

About Horizon3.ai

The NodeZero™ platform empowers organizations to continuously find, fix, and verify exploitable attack surfaces. It is the flagship product of Horizon3.ai, founded in 2019 by former industry and U.S. National Security veterans. Our mission is to help organizations see their networks through the eyes of the attacker and proactively fix problems that truly matter, improve the effectiveness of their security initiatives, and ensure that they are prepared to respond to real cyberattacks.

Follow Horizon3.ai: LinkedIn and on X, formerly known as Twitter.

Contact: Horizon3.AI Europe GmbH,
Sebastian-Kneipp-Straße 41, 60439 Frankfurt am Main, Germany,
Web: www.horizon3.ai

PR-agency: euromarcom public relations GmbH,
Muehlhohle 2, 65205 Wiesbaden, Germany,
Tel.: +49 611 973150, E-Mail: team@euromarcom.de,
Web: www.euromarcom.de

- - - -