VulNow Becomes a CVE Numbering Authority under ENISA Root

Predictive vulnerability threat intelligence platform secures CNA status under ENISA Root.

AMSTERDAM, NETHERLANDS – June 30, 2026 – VulNow B.V., a predictive software supply chain risk intelligence platform, today announced its formal appointment as a CVE™ (Common Vulnerabilities and Exposures) Numbering Authority (CNA) under the European Union Agency for Cybersecurity (ENISA) CVE Root. This designation formalizes VulNow's coordinated vulnerability disclosure pipeline, authorizing the company to directly assign CVE identifiers (CVE IDs) to vulnerabilities discovered via its predictive intelligence engine for proprietary products and third-party open source vulnerabilities that are not already covered under the scope of another CNA.

Shifting from Reactive to Predictive Vulnerability Management

Traditional vulnerability management programs face a critical signal problem. VulNow provides PreCVE signal intelligence that standard scanners cannot detect before a CVE ID is formally published. During a coordinated disclosure window, organizations with the VulNow intelligence integrated into their platforms and tools gain exclusive visibility into these PreCVEs. Following a coordinated disclosure process, VulNow will publish the official CVE Record on behalf of open source maintainers (that are not CNAs themselves) to enable public remediation.

Exposing Dark Matter Vulnerabilities™

Partnering with the CVE Program allows VulNow to systematically bring a critical category of risk into the public record. The VulNow platform is designed to target Dark Matter Vulnerabilities™, which are security flaws that have been quietly patched or incidentally resolved in code repositories by maintainers without the correlated publication of a public CVE ID or security advisory. Because standard enterprise vulnerability scanners rely entirely on published CVE databases, these unindexed code changes remain completely invisible to security teams while remaining exposed to threat actors who reverse engineer open source software.

"Securing CNA status under the ENISA Root is a structural milestone for our company, our customers, and our partners with security solutions," said Cassie Crossley, CEO and Co-Founder of VulNow. "Standard vulnerability scanners are blind to Dark Matter Vulnerabilities™ because they rely exclusively on post-disclosure CVE feeds. By formalizing our disclosure workflow as a CNA, we can rapidly move our deep queue of active PreCVE intelligence into the public record, shortening the window of attacker opportunity and helping our customers and partners achieve proactive compliance ahead of the EU CRA vulnerability reporting timeline and broader 2027 compliance obligations."

Validated Operational Telemetry

The VulNow Q1 2026 Threat Intelligence Report details the production capabilities of this pipeline. During the first quarter of 2026, VulNow confirmed a subset of 58 PreCVE detections that successfully resolved to published CVE Records. The platform delivered an average early warning lead time of 6.6 days across a monitored subset of core open source packages representing a combined download volume of 13.2 billion monthly installations.

The report highlights a maximum predictive window of 154 days and 15 hours for a vulnerability (CVE-2026-39865) in the axios open source project, demonstrating the platform's ability to identify risk months before traditional signature availability. CNA status allows VulNow to transition these early signals into actionable, registered advisories at scale, with confirmed PreCVEs accessible at https://vul.now/precve.

Open source maintainers and vulnerability disclosure programs can review reporting protocols and submission guidelines by visiting the VulNow Coordinated Vulnerability Disclosure policy.

About the CVE Program

The mission of the CVE™ Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.

About VulNow B.V.

Headquartered in the Netherlands, VulNow B.V. provides predictive threat intelligence designed for modern software supply chain risk management. By leveraging advanced machine learning to detect undisclosed vulnerabilities, silent patches, and Dark Matter Vulnerabilities™ prior to public advisory publication, VulNow delivers early-warning telemetry to enterprise defenders and strategic infrastructure operators.

Media Contact:

VulNow B.V.

info@vul.now

https://vul.now