



Why Vulnerability Scanning is a Top Cyber Threat: ShadowSyndicate

ShadowSyndicate is casting a wide net in searching for vulnerabilities within servers by deploying automated scanners across the internet. Currently the cybercrime group is utilizing these scanners to hunt for devices running outdated versions of aiohttp (anything before 3.9.2). They can identify targets either by searching for specific characteristics associated with aiohttp or by attempting to exploit the vulnerability itself and analyzing the server's response.

The public availability of a proof-of-concept exploit for CVE-2024-23334 gives ShadowSyndicate a blueprint for crafting their attack. They can leverage this code or develop their own variation to trick vulnerable servers into granting unauthorized access. Once a vulnerable system is identified, ShadowSyndicate might target specific files containing sensitive data, such as user databases, password lists, or critical system configurations. By successfully exploiting the vulnerability, they could gain an initial foothold on the system, potentially allowing them to upload additional tools or deploy their ransomware payload.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.