

Forum:[Hack Forums](#)

Thread: [CISA Releases Advisory on Lessons Learned from an Incident Response Engagement](#)

Stanley - October 11, 2025, 12:20 am

CISA Releases Advisory on Lessons Learned from an Incident Response Engagement

Today, CISA released a cybersecurity advisory detailing lessons learned from an incident response engagement following the detection of potential malicious activity identified through security alerts generated by the agency's endpoint detection and response tool.

This advisory, CISA Shares Lessons Learned from an Incident Response Engagement, highlights takeaways that illuminate the urgent need for timely patching, comprehensive incident response planning, and proactive threat monitoring to mitigate risks from similar vulnerabilities.

The advisory also outlines the tactics, techniques, and procedures (TTPs) employed by cyber threat actors, including exploitation of GeoServer Vulnerability CVE-2024-36401 for initial access. By understanding these TTPs, organizations can enhance their defenses against similar threats.

CISA recommends organizations take the following actions:

Prioritize Patch Management: Expedite patching of critical vulnerabilities, particularly those listed in CISA's Known Exploited Vulnerabilities catalog, with a focus on public-facing systems.

Strengthen Incident Response Plans: Regularly update, test, and maintain incident response plans, ensuring they include procedures for engaging third-party responders and deploying security tools without delay.

Enhance Threat Monitoring: Implement centralized, out-of-band logging and ensure security operations centers continuously monitor and investigate abnormal network activity to detect and respond to malicious activity effectively.

CISA urges organizations to apply these lessons learned to bolster their security posture, improve preparedness, and reduce the risk of future compromises. For additional details, review the full cybersecurity advisory.

<https://www.cisa.gov/news-events/alerts/2025/09/23/cisa-releases-advisory-lessons-learned-incident-response-engagement>

Vectura - October 11, 2025, 1:22 am

Another case proving that delayed patching is one of the biggest security gaps out there. Lessons like these are worth acting on, not just reading.

Aeowulf - October 11, 2025, 5:50 am

I've seen a lot from CISA lately... just as Trump is trying to fire CISA workers.

JoshAllen - October 11, 2025, 6:15 am

I'm shocked they even have to suggest "Prioritize Patch Management"

Shouldn't that always be the main priority?