EINPRESSWIRE

Clutch Security Uncovers How Attackers Exploit Secrets in Seconds, Exposing the Flaws in Rotation Practices

Evidence-based research reveals how attackers rapidly discover and exploit exposed secrets, with compromises occurring in mere seconds.

Clutch Logo

TEL-AVIV, ISRAEL, December 2, 2024 /EINPresswire.com/ -- Clutch Security, a leading innovator in Non-Human Identity (NHI) security and management, today released groundbreaking research challenging the effectiveness of traditional secret rotation practices. The study uncovers how attackers—using automated tools—exploit leaked NHIs faster than organizations can respond, with some compromises occurring in under a minute.

For years, secret rotation has been a cybersecurity staple, with API keys, tokens, service accounts, certificates, and other credentials rotated on intervals of 120, 90, or even 30 days. But Clutch's research reveals this practice now creates inefficiencies and a false sense of security, leaving organizations vulnerable to rapidly evolving threats.

> “
> Attackers are moving at machine speed, and outdated playbooks aren't keeping up. Even the best security processes can't compete once a secret is exposed. We need to rethink our defenses.”
>
> *Ofir Har-Chen, Co-founder and CEO of Clutch Security*

Key Findings
Clutch's research team conducted controlled experiments, intentionally leaking various NHIs across platforms including cloud environments, SaaS applications, CI/CD pipelines, and developer forums. The results are alarming:
Compromise in Seconds: On high-traffic platforms, exposed secrets were exploited within seconds, with unauthorized activity spiking during early morning UTC hours.

Rotation’s Failures: Secrets rotated hourly and re-leaked were still compromised at the same rate, proving attackers act faster than even aggressive rotation schedules.
GitHub is Hotspot: Credentials leaked on GitHub were often accessed almost immediately, with attackers deploying bots to scrape for exposed secrets.
Sophisticated Exploits: Attackers used exposed secrets to escalate privileges and pivot laterally, showcasing their advanced and highly organized techniques.

The False Promise of Rotation

Secret rotation remains a compliance checkbox for many organizations, but Clutch’s findings expose its limitations. The gap between exposure and rotation—often days, weeks, or months—is more than enough for attackers to inflict damage. Worse, over-reliance on rotation fosters complacency, creating blind spots in overall security strategies.

These findings align with the updated NIST guidelines (SP 800-63B), which recommend against periodic password changes unless there’s evidence of compromise. This shift reflects a broader industry awakening: traditional security measures are falling short against modern threats.

A Call to Action

“Attackers are moving at machine speed, and outdated playbooks aren’t keeping up,” said Ofir Har-Chen, Co-founder and CEO of Clutch Security. “Even the best security processes can’t compete once a secret is exposed. We need to rethink our defenses, focusing on proactive measures like Zero Trust architectures and ephemeral identities to shrink the attack surface and limit damage.”

To support this shift, Clutch has introduced community-focused tools like AWSKeyLockdown, an open-source solution enabling teams to instantly revoke exposed AWS access keys, cutting attackers off before they can exploit them. “If tools like this can stop even one compromise, we’ve done our job,” Har-Chen added.

Click here to read the full research.

About Clutch Security

In today’s digital world, enterprises face enormous challenges in managing and securing Non-Human Identities (NHIs) at scale. Clutch Security’s Universal NHI Security Platform empowers organizations to understand, control, and protect NHIs across their ecosystems. With industry-first Zero Trust-based solution, Clutch provides unparalleled visibility, context-driven insights, and proactive protections for mission-critical NHIs.

Learn more at clutch.security.

Tom Sadon
Clutch Security
tom@clutch.security