AL2025_39 PyPI Invalidates Tokens Stolen in GhostAction Supply Chain Attack (September 23rd, 2025)

Description

In September 2025, the Python Software Foundation (PSF) canceled all PyPI tokens stolen in the GhostAction attack. These tokens, which let developers publish packages on PyPI, were taken through malicious GitHub Actions workflows. Luckily, investigators found no signs that the attackers used them to upload harmful packages.

Attack Details

On September 5th, GitGuardian reported malicious GitHub Actions workflows (e.g., *FastUUID*) attempting to steal PyPI tokens. A delayed response due to a missed email allowed attackers to compromise over 3,300 secrets across multiple platforms (PyPI, npm, DockerHub, GitHub, Cloudflare, AWS, and databases). More than 570 repositories were affected, with some companies' SDK portfolios fully exposed. PyPI, led by Mike Fiedler (a PyPI administrator and security engineer with the Python Software Foundation), invalidated all stolen tokens and advised maintainers to switch to short-lived Trusted Publishers tokens for better protection.

Remediation

- **Use of Trusted Publishers**: Maintainers are urged to adopt short-lived tokens via Trusted Publishers with GitHub Actions.
- **Repository Audit**: Project maintainers should review GitHub Actions workflows, rotate tokens, and ensure secnsitive data is not hard-coded.
- **Security Monitoring**: Maintain vigilant monitoring of account security logs for suspicious activity.
- **Cross-Ecosystem Review**: Given that other ecosystems (npm, Rust crates, DockerHub) were also targeted, organizations should check for compromise across all package registries.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Bleeping Computer, PyPI invalidates tokens stolen in GhostAction supply chain attack (September 18th, 2025). Red River. https://www.bleepingcomputer.com/news/security/pypi-invalidates-tokens-stolen-in-ghostaction-supply-chain-attack/
- Secure Blink, PyPI Shuts Down Stolen Tokens After Massive GhostAction Supply Chain Attack. (September 18th, 2025). Retrieved from Secure Blink.

https://www.secureblink.com/cyber-security-news/py-pi-shuts-down-stolen-tokens-after-massive-ghost-action-supply-chain-attack