#1 Trusted Cybersecurity News Platform

The Hacker News

GitHub Vulnerability 'ArtiPACKED' Exposes Repositories to Potential Takeover

Ravie Lakshmanan Aug 15, 2024

A newly discovered attack vector in GitHub Actions artifacts dubbed **ArtiPACKED** could be exploited to take over repositories and gain access to organizations' cloud environments.

"A combination of misconfigurations and security flaws can make artifacts leak tokens, both of third party cloud services and GitHub tokens, making them available for anyone with read access to the repository to consume," Palo Alto Networks Unit 42 researcher Yaron Avital said in a report published this week.

"This allows malicious actors with access to these artifacts the potential of compromising the services to which these secrets grant access."

The cybersecurity company said it primarily observed the leakage of GitHub tokens (e.g., GITHUB_TOKEN and ACTIONS_RUNTIME_TOKEN), which could not only give malicious actors unauthorized access to the repositories, but also grant them the ability to poison the source code and get it pushed to production via CI/CD workflows.

Artifacts in GitHub allow users to share data between jobs in a workflow and persist that information after it has been completed for 90 days. This can include builds, log files, core dumps, test outputs, and deployment packages.

The security problem here is that these artifacts are publicly available for anyone in the case of open-source projects, making them a valuable resource for extracting secrets like GitHub access tokens.

Particularly, the artifacts have been found to expose an undocumented environment variable called ACTIONS_RUNTIME_TOKEN, which has a lifespan of about six hours and could be used to substitute an artifact with a malicious version before it expires.

This could then open an attack window for remote code execution when developers directly download and execute the rogue artifact or there exists a subsequent workflow job that's configured to run based on previously uploaded artifacts.

While GITHUB_TOKEN expires when the job ends, improvements made to the artifacts feature with version 4 meant that an attacker could exploit race condition scenarios to steal and use the token by downloading an artifact while a workflow run is in progress.

The pilfered token could be subsequently used to push malicious code to the repository by creating a new branch before the pipeline job ends and the token is invalidated. However, this attack banks on the workflow having the "contents: write" permission.

An important point to note here is that the GitHub tokens aren't part of the repository code but are only exposed when a CI/CD pipeline is triggered and an artifact containing the tokens is uploaded, thereby allowing an attacker to download the artifact, access the token, and use it to inject nefarious code to the repository.

A number of open-source repositories related to Amazon Web Services (AWS), Google, Microsoft, Red Hat, and Ubuntu have been found susceptible to the attack. GitHub, for its part, has categorized the issue as informational, requiring that users take it upon themselves to secure their uploaded artifacts.

"GitHub's deprecation of Artifacts V3 should prompt organizations using the artifacts mechanism to reevaluate the way they use it," Avital said. "Overlooked elements like build artifacts often become prime targets for attackers."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

— Latest News

Cybersecurity Resources

Uncover Identity Dark Matter: SACR Research Brief

Earn a Master's in Cybersecurity Risk Management

Your VPN is Helping Attackers Move as Fast as AI

Zscaler ThreatLabz 2026 VPN Risk Report with Cybersecurity Insiders.

Expert Insights

Videos Articles

Why Security Leaders Are Layering Email Defense on Top of Secure Email Gateways

Session Cookie Theft: You Showed Your ID at the Door. But Someone Else Has Your Room Key

Why AI Does Not Need to be Innovative to be Dangerous

AI Will Change Cybersecurity. Humans Will Define Its Success. A Lesson No Algorithm Can Teach

Get Latest News in Your Inbox

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders – all for free.

Your e-mail address

Connect with us!

Company

About THN
Advertise with us
Contact

Pages

Webinars
Awards
Privacy Policy

Contact Us