Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

LeakyCLI Vulnerability in Cloud Tools Puts Credentials at Risk

Date of Publication	Admiralty Code	TA Number
April 18, 2024	A1	TA2024152

Summary

First Seen: 2023
Affected Platform: AWS CLI and Google Cloud CLI
Impact: A security vulnerability named LeakyCLI that can expose sensitive information in cloud computing environments. This vulnerability is present in cloud command line tools and can expose serverless environment variables. If exploited by attackers, this vulnerability can lead to them gaining access to credentials.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
Unassigned	AWS CLI and Google Cloud CLI Command Information Disclosure Vulnerability	AWS CLI and Google Cloud CLI	✗	✗	✗
CVE-2023-36052	Microsoft Azure CLI REST Command Information Disclosure Vulnerability	Microsoft Azure	✗	✗	✓

Vulnerability Details

#1 A security vulnerability named LeakyCLI that can expose sensitive credentials in cloud computing environments. The vulnerability affects certain cloud command-line interface (CLI) tools used with AWS and Google Cloud Platform.

#2 These CLI tools can leak sensitive information present in environment variables, if not handled properly. Leaked credentials can be potentially accessed by attackers if the build logs are published through tools like GitHub Actions.

#3 The issue resembles one Microsoft faced with Azure CLI, known as CVE-2023-36052, and addressed through updates. The CLI vulnerability, often integrated into CI/CD pipelines, bypasses secret labeling and can divulge passwords, usernames, and keys, potentially compromising resources.

#4 Proof-of-concept searches on GitHub repositories, uncovering numerous instances of sensitive data exposure through environment variables, which could lead to significant security breaches if exploited.

#5 In essence, LeakyCLI highlights the risk of exposing sensitive credentials in build logs if proper caution isn't exercised with CLI tools for cloud platforms. To mitigate this risk, it is recommended to storing secrets in a dedicated secrets store service rather than environment variables.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
Unassigned	AWS CLI and Google Cloud CLI	cpe:2.3:o:aws:aws_cli:*:*:*:*:*:*:*:* cpe:2.3:o:google:google_cloud_cli:*:*:*:*:*:*:*:*	CWE-200
CVE-2023-36052	az webapp config appsettings set & delete: All versions; az staticwebapp appsettings set & delete: All versions; az logicapp config appsettings set & delete: All versions; az functionapp config appsettings set & delete: All versions	cpe:2.3:a:microsoft:az_webapp_config_appsettings_set:*:*:*:*:*:*:*:*	CWE-200

Recommendations

Avoid Storing Secrets in Environment Variables: Refrain from storing sensitive information such as passwords, usernames, and keys in environment variables within serverless resources. Instead, opt for using dedicated secrets management services provided by your cloud service provider (CSP), such as AWS Secrets Manager or Google Cloud Secrets Manager.

Review and Suppress Command Outputs: Regularly review the contents of your build logs to identify and mitigate any potential exposure of sensitive information. Consider suppressing command outputs that are not necessary for debugging or monitoring purposes by piping them to /dev/null. This practice helps prevent unnecessary exposure of sensitive data in logs.

Update CLI Tools: Keep CLI tools up to date with the latest versions provided by the respective cloud service providers. Updates often include security patches and enhancements that address known vulnerabilities and improve overall security posture.

Implement Access Controls: Implement appropriate access controls to restrict access to sensitive information, including build logs and secret management services. Limit access to authorized personnel and ensure permissions are scoped appropriately based on job roles and responsibilities.

Vulnerability Scanning: Conduct regular vulnerability scans on your network to identify any potential weaknesses or unpatched software. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0006** Credential Access	**TA0043** Reconnaissance	**TA0009** Collection
TA0042 Resource Development	**T1552** Unsecured Credentials	**T1078** Valid Accounts	**T1190** Exploit Public-Facing Application
T1530 Data from Cloud Storage	**T1552.001** Credentials In Files	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36052

References

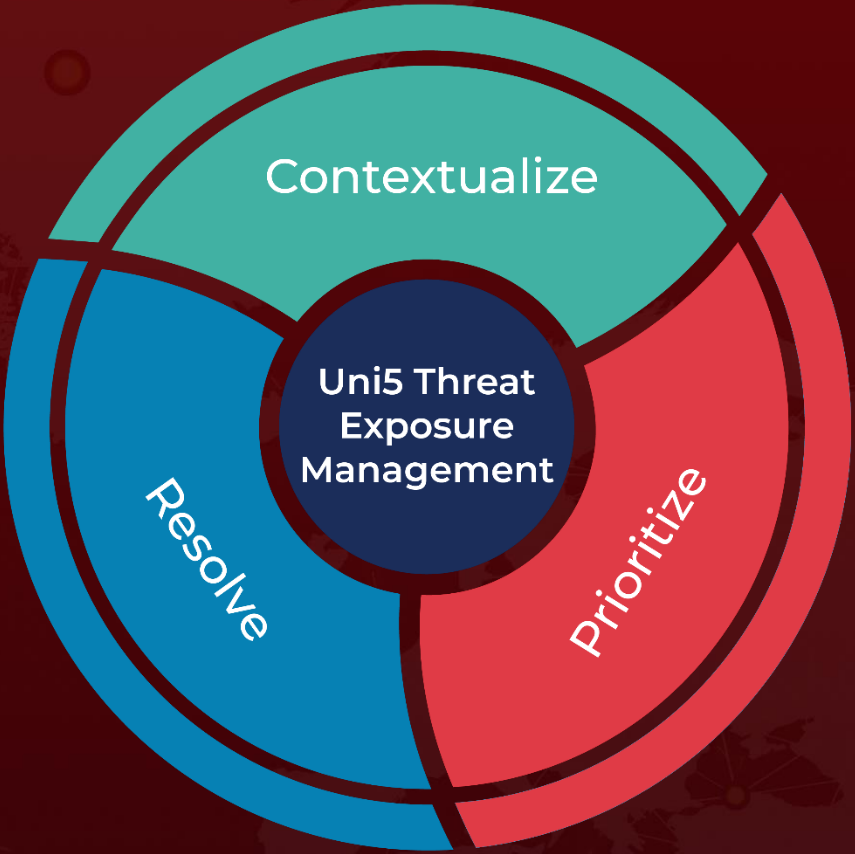
https://orca.security/resources/blog/leakycli-aws-google-cloud-command-line-tools-can-expose-sensitive-credentials-build-logs/

https://www.hivepro.com/threat-advisory/microsofts-november-2023-patch-tuesday-addresses-five-zero-day-vulnerabilities/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 18, 2024 • 4:30 AM

More at www.hivepro.com