Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

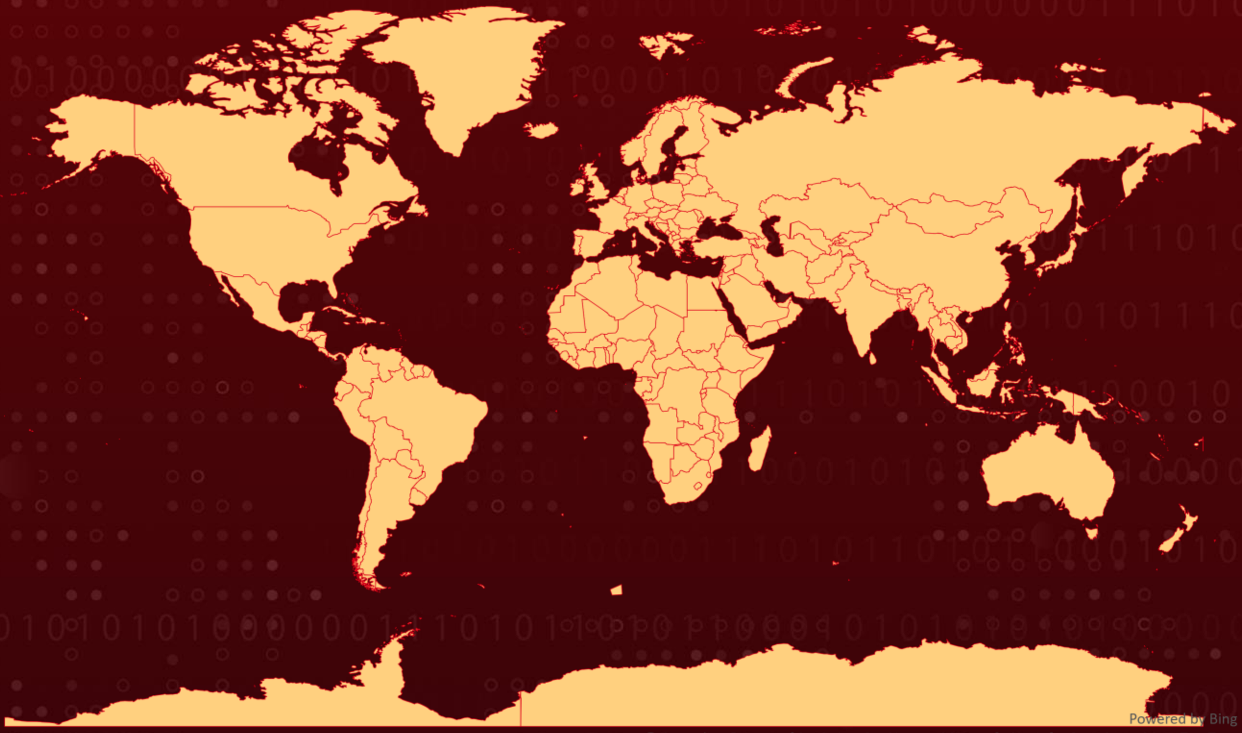
A new EmojiDeploy attack has been found in an Azure service

Date of Publication	Admiralty Code	TA Number
January 20, 2023	A1	TA2023037

Summary

First appeared: October 26, 2022
Attack Region: Worldwide
Affected Services: Azure Functions, Azure App Service, Azure Logic Apps, and other services that use Kudu
Attack: EmojiDeploy allows for remote code execution and deployment of malicious zip files through cross-site request forgery (CSRF) on the Azure SCM service Kudu.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

The EmojiDeploy attack chain allows a threat actor to run arbitrary code, steal or delete sensitive data, and compromise a targeted application on Azure by exploiting a remote code execution vulnerability through cross-site request forgery (CSRF) on the SCM service Kudu. The attack uses a misconfigured cookie setting for the Source Code Manager (SCM) service on Azure, which sets two controls to default "Lax."

#2

This vulnerability affects Azure App Service, Azure Functions, and Azure Logic Apps. The attack highlights the lack of visibility into what cloud platforms do under the hood, which undermines their security, and cloud providers need to make their security controls more transparent and default to more secure configurations.

#3

The vulnerability has been fully remediated but organizations can defend against similar vulnerabilities in the future by effectively applying the principle of least privilege and being aware of the SCM panel and its capabilities.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IOCs)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation	TA0008 Lateral Movement
TA0005 Defense Evasion	TA0042 Resource Development	TA0006 Credential Access	TA0009 Collection
TA0011 Command and Control	T1566 Phishing	T1204 User Execution	T1204.002 Malicious File
T1059 Command and Scripting Interpreter	T1216 System Script Proxy Execution	T1189 Drive-by Compromise	T1068 Exploitation for Privilege Escalation
T1071 Application Layer Protocol	T1071.001 Web Protocol	T1203 Exploitation for Client Execution	T1588 Obtain Capabilities
T1530 Data from Cloud Storage	T1584 Compromise Infrastructure	T1606 Forge Web Credentials	T1606.001 Web Cookies
T1602 Data from Configuration Repository	T1406 Obfuscated Files or Information		

References

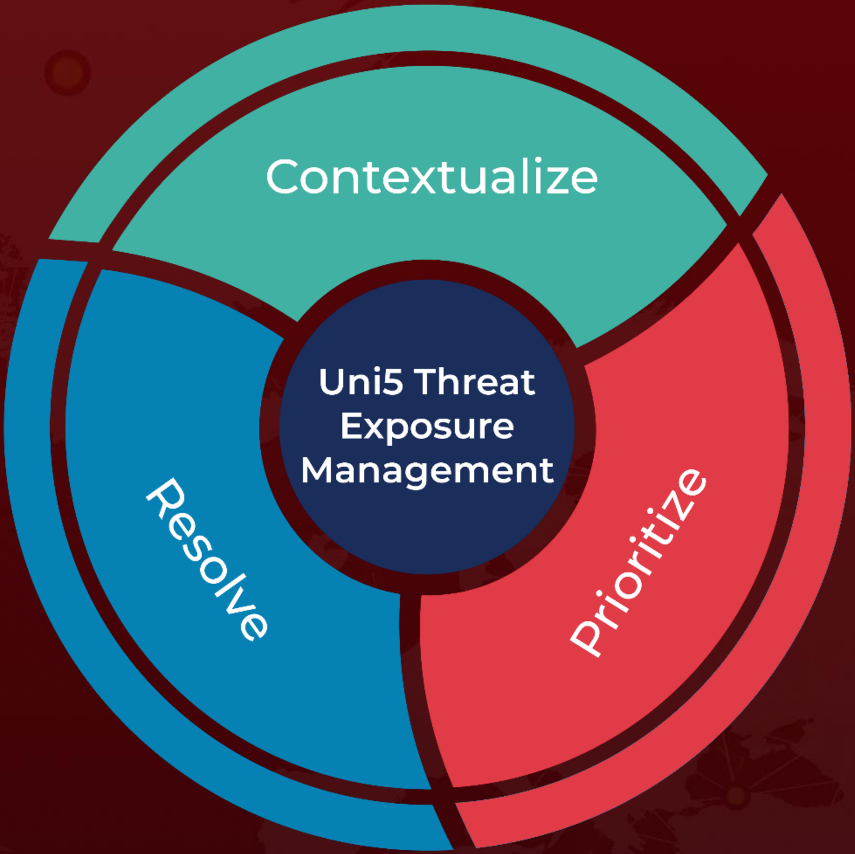
https://ermetic.com/blog/azure/emojideploy-smile-your-azure-web-service-just-got-rced/

https://www.darkreading.com/cloud/emojideploy-attack-chain-targets-misconfigured-azure-service

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

January 20, 2023 • 6:45 AM

More at www.hivepro.com