

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Cracking ShellTorch Vulnerabilities: Exposing TorchServe to RCE

Date of Publication

October 5, 2023

Admiralty Code

A1

TA Number

TA2023399

Summary










First Seen: October 2, 2023

Affected Product: TorchServe

Affected Commercial Users: Amazon, OpenAI, Tesla, Azure, Google, Walmart, and Intel

Impact: A trio of security vulnerabilities, dubbed 'ShellTorch,' in the open-source machine-learning model TorchServe, a tool for serving and scaling PyTorch models, could be chained to achieve remote code execution on affected systems, potentially leading to server takeover. There are numerous instances of TorchServe found publicly exposed on the internet, comprising thousands, and among them are servers affiliated with some of the globe's largest and most distinguished organizations.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
Unassigned	Unauthenticated Management Interface API Misconfiguration Vulnerability	TorchServe			
CVE-2023-43654	Remote Server-Side Request Forgery (SSRF) Vulnerability	TorchServe			
CVE-2022-1471	Java Deserialization RCE Vulnerability	TorchServe			

Vulnerability Details

#1

A suite of pivotal vulnerabilities within the PyTorch Model Server has raised concerns in the artificial intelligence (AI) and machine learning (ML) community. If these vulnerabilities are chained and exploited, they could serve as a gateway to remote code execution and potential server takeovers. Situated at the intersection of AI models and open-source software (OSS) libraries, the PyTorch library stands as one of the world's most widely utilized machine learning frameworks.

#2

The trusted open-source TorchServe library boasts global adoption, evident in its impressive metrics of over 30,000 PyPi downloads monthly and exceeding a million total DockerHub pulls. Notably, major corporations, including industry giants like Walmart, Amazon, OpenAI, Tesla, Azure, Google Cloud, and Intel, among others, rely on TorchServe for their operations. Moreover, TorchServe serves as the foundation for influential projects such as KubeFlow, MLFlow, Kserve, AWS Neuron, and more.

#3

A triad of security vulnerabilities in TorchServe, collectively named "ShellTorch," exposes critical risks. The initial vulnerability involves an unauthenticated misconfiguration in the management interface API. This flaw defaults the web panel binding to the IP address 0.0.0.0 instead of localhost, leaving it vulnerable to external requests. The absence of authentication in this interface grants unrestricted access, allowing any user to upload malicious models from an external source.

#4

The second issue, identified as CVE-2023-43654, presents a remote server-side request forgery (SSRF). When exploited in conjunction with the aforementioned vulnerability, an attacker gains access to the management server remotely, facilitating remote code execution without authentication on any default TorchServe server. This SSRF flaw serves as an independent attack vector and can also trigger an additional unsafe deserialization RCE vulnerability (CVE-2022-1471). This particular vulnerability, rooted in a Java deserialization issue, permits remote code execution.

#5

Affected versions of TorchServe that utilize the SnakeYAML open-source library are susceptible to exploitation through insecure deserialization. By exploiting vulnerabilities in the SnakeYAML library, attackers can upload a model with a malicious YAML file, triggering remote code execution. This amalgamation of vulnerabilities empowers the remote execution of code with elevated privileges, all without requiring authentication. Consequently, it enables unauthorized access to view, modify, steal, and delete AI models and sensitive data traversing to and from the targeted TorchServe server.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
Unassigned	TorchServe: 0.1.0 - 0.8.1	cpe:2.3:a:pytorch:torchserve:*:*:*:*:*	CWE-862
CVE-2023-43654			CWE-918
CVE-2022-1471		cpe:2.3:a:snakeyaml:project:snakeyaml:*:*:*:*:*	CWE-502 CWE-20

Recommendations



Update TorchServe to Version 0.8.2: Ensure that your TorchServe version is upgraded to at least 0.8.2. It's crucial to note that this update, while significant, adds a warning to TorchServe without addressing the SSRF vulnerability.



Securely Configure the Management Console: Minimizing potential impacts by correctly configuring the management console prevents attackers from exploiting default settings to access the management console remotely. Implement a fix by setting your config.properties file:
management_address: http://127.0.0.1:8081



Restrict Model Fetching to Trusted Domains: Enhance your server's security by permitting model fetching exclusively from trusted domains. Update your config.properties file and adjust the URLs according to your specific requirements:
allowed_urls=https://s3.amazonaws.com/.*,https://torchserve.pytorch.org/.*



Identify and Address Impacted Instances: Given the widespread impact with tens of thousands of instances affected, it's crucial to assess whether your organization is using vulnerable versions of TorchServe. Utilize the [ShellTorch Checker Tool](#) to identify and address potentially compromised instances.



Vulnerability Management: This entails routinely assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches. Evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0004</u> Privilege Escalation
<u>TA0005</u> Defense Evasion	<u>TA0007</u> Discovery	<u>TA0008</u> Lateral Movement	<u>TA0009</u> Collection
<u>TA0011</u> Command and Control	<u>T1059</u> Command and Scripting Interpreter	<u>T1090</u> Proxy	<u>T1505</u> Server Software Component
<u>T1135</u> Network Share Discovery	<u>T1005</u> Data from Local System	<u>T1133</u> External Remote Services	<u>T1105</u> Ingress Tool Transfer
<u>T1068</u> Exploitation for Privilege Escalation	<u>T1055</u> Process Injection	<u>T1588.006</u> Vulnerabilities	<u>T1588</u> Obtain Capabilities

Patch Links

<https://github.com/pytorch/serve/security/advisories/GHSA-8fxr-qfr9-p34w>

<https://bitbucket.org/snakeyaml/snakeyaml/issues/561/cve-2022-1471-vulnerability-in#comment-64581479>

References

<https://www.oligo.security/blog/shelltorch-torchserve-ssrf-vulnerability-cve-2023-43654>

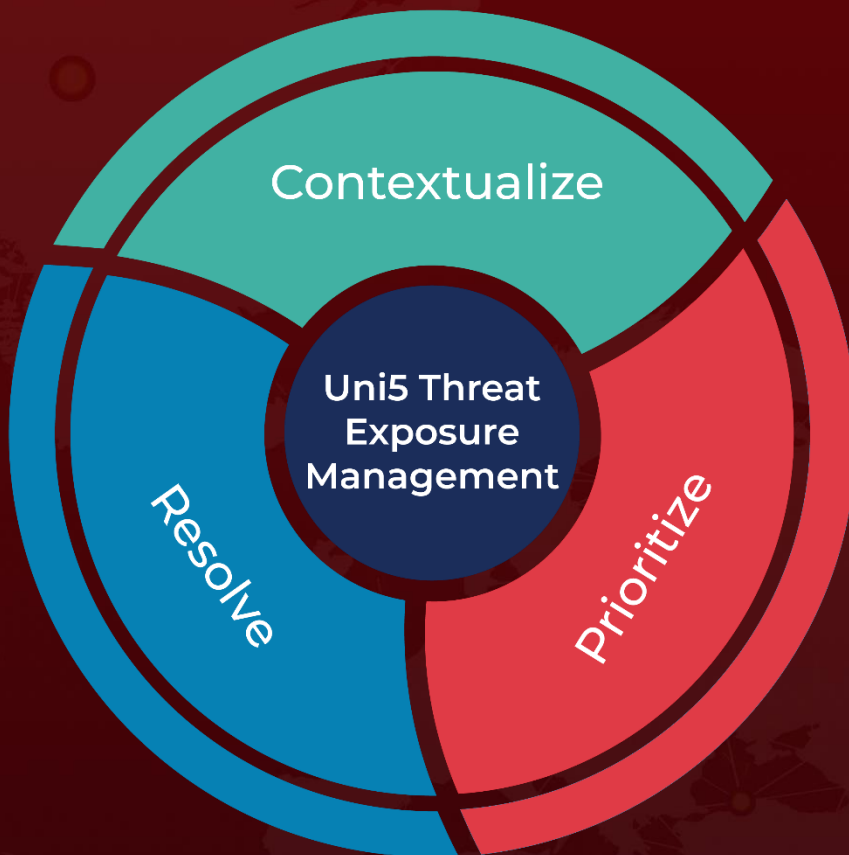
<https://aws.amazon.com/security/security-bulletins/AWS-2023-009/>

<https://github.com/OligoCyberSecurity/ShellTorchChecker>

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

October 5, 2023 • 7:00 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com