مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in PyTorch

Tracking #:432315945

Date:11-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Critical vulnerability in PyTorch that could be exploited to execute malicious code on vulnerable systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-5480**
- CVSS Score: 10 Critical
- Remote code execution (RCE) vulnerability exists in PyTorch's torch.distributed.rpc framework. This framework is used for distributed training in machine learning applications.
- The vulnerability arises from the framework's inadequate verification of functions called during Remote Procedure Calls (RPC). Attackers can exploit this by sending a specially crafted Python User Defined Function (UDF) to the master node during multi-CPU RPC communication. The master node deserializes and executes the UDF without proper validation, allowing attackers to run arbitrary code on the system.
- Successful exploitation of this vulnerability allows remote attackers to execute arbitrary commands on compromised machines. In the context of PyTorch, this could lead to the compromise of master nodes initiating distributed training and the theft of sensitive AI data.

Affected Versions:

- PyTorch versions prior to 2.2.2

Fixed Versions:

- PyTorch versions 2.3.1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by PyTorch

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-5480