Black Duck Security Advisory

PyTorch Vulnerable to Remote Code Execution (RCE) via Command Injection in 'torch.distributed.rpc' framework

BDSA | BDSA-2024-3458 | CVE-2024-5480 | **Published** Jun 7, 2024 | **Updated** Sep 27, 2024

This vulnerability is currently under review with Black Duck.

HIGH 8.7	No Fix	Exploit Available	119 Days
BDSA		Jun 5, 2024	Vulnerability Age

PyTorch is vulnerable to remote code execution (RCE) via command injection within the `torch.distributed.rpc` framework. An attacker could exploit this in order to remotely attack master nodes that are starting distributed training.

Zero-click Remote Code Execution

This vulnerability can result in the execution of code on the system, triggered by a remote attacker without requiring or relying on any third party action.

How to fix it

No Solution

No Workaround

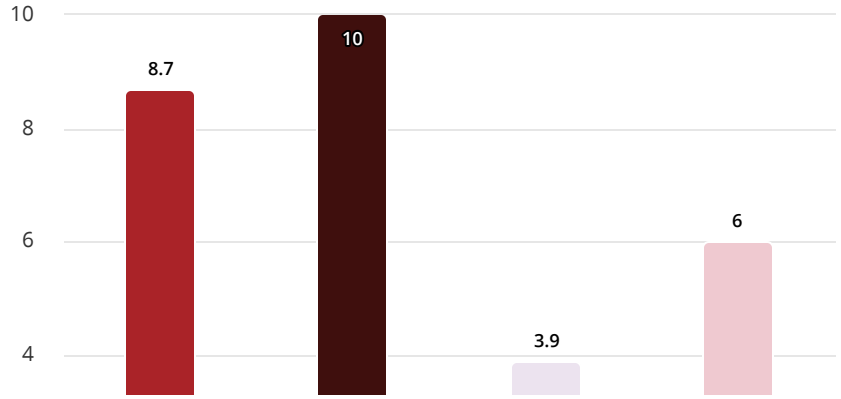
Scores and Metrics

Scores for the related BDSA and NVD records, based on the Common Vulnerability Scoring System (CVSS).

CVSS v2 | CVSS v3.x

This Record	Related Record
BDSA-2024-3458	**CVE-2024-5480**
CVSS v3.x	CVSS v3.x

Overall **8.7 High**



CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:U/RC:U

Temporal **8.7 High**

Exploitability

Not Defined | Unproven | **Proof of Concept** | Functional | High

Remediation Level

Not Defined | Official Fix | Temporary Fix | Workaround | **Unavailable**

Report Confidence

Not Defined | **Unknown** | Reasonable | Confirmed

Exploitability **3.9 Low**

Attack Vector

Overall **N/A**

No score data available.

Temporal **N/A**

NVD does not provide Temporal metrics.

Exploitability **N/A**

Exploitability metrics are not available.

Network Adjacent Network Local Physical	
Attack Complexity	
Low High	
Privileges Required	
None Low High	
User Interaction	
None Required	
Scope	
Unchanged **Changed**	
Impact **6** Medium	Impact **N/A**
Confidentiality Impact	*Impact metrics are not available.*
None Low **High**	
Integrity Impact	
None Low **High**	
Availability Impact	
None Low **High**	

Common Weakness Enumeration (CWE)

CWE-77 - Improper Neutralization of Special Elements used in a Command ('Command Injection')

The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component.