

Forum:[Hack Forums](#)

Thread: [ChatGPT Vulnerability Actively Exploited from Over 10,000 IPs to Target US Government](#)

JoseMar - March 18, 2025, 7:51 am

ChatGPT Vulnerability Actively Exploited from Over 10,000 IPs to Target US Government Organizations

Aggressors are effectively misusing a Server-Side Ask Imitation (SSRF) defenselessness in OpenAI's ChatGPT foundation. The powerlessness, as distinguished as CVE-2024-27564, has ended up being a critical danger in spite of its medium seriousness classification.

According to an inquiry by cybersecurity firm Veriti, this defenselessness has, as of now, been weaponized in various real-world assaults, illustrating how risk-performing artists can indeed use direct security imperfections to compromise modern AI systems.

Massive Scale of Exploitation

The scale of these assaults is especially disturbing. Verity's inquiry revealed over 10,479 assault endeavors beginning from a pernicious IP address inside the fair one week.

These numbers propose a facilitated and determined campaign focusing on organizations utilizing OpenAI's innovation.

The United States has experienced the most elevated concentration of assaults at 33%, with Germany and Thailand taking after at 7% each.

Top assaults executed

Other influenced locales incorporate Indonesia, Colombia, and the Joined Together Kingdom, demonstrating the worldwide scope of this threat.

"This attack pattern demonstrates that no vulnerability is too small to matter – attackers will exploit any weakness they can find" famous analysts in their report.

The abuse slant appears to surge in January 2025, followed by a diminish in February and Walk, conceivably showing attackers' moving strategies or reactions to security measures.

Server-side Ask Imitation Vulnerability

CVE-2024-27564 is classified as a server-side ask imitation defenselessness, permitting aggressors to infuse noxious URLs into input parameters.

This method strengthens ChatGPT's application to make unintended demands for the attacker's sake. SSRF vulnerabilities regularly happen when client input information is utilized to create an ask without legitimate approval.

In this case, aggressors can control parameters to control demands from other servers or, indeed, the same server.

The powerlessness unequivocally influences the pictureproxy.php component of ChatGPT, as distinguished in commit f9f4bbc.

By controlling the 'URL' parameter, aggressors can start self-assertive demands, possibly bypassing security controls.

Recommendations Review and rectify IPS, WAF, and firewall arrangements to guarantee security against CVE-2024-27564.

- Implement strict input approval to avoid malevolent URL injection.

- Monitor logs for assault endeavors from known pernicious IP addresses.

- Consider organizing division to confine components dealing with URL fetching.

- Prioritize AI-related security crevices in chance evaluation procedures.

This occurrence speaks to another illustration of state-sponsored and criminal risk-performing artists progressively focusing on AI frameworks for malevolent purposes.

As uncovered in a later report, aggressors have endeavored to abuse ChatGPT for hurtful exercises in more than 20 occurrences since early 2024.

The abuse of CVE-2024-27564 serves as a stark update that, indeed, medium-severity vulnerabilities can pose noteworthy dangers when weaponized by decided aggressors.

Additional sources to explore: You can also search directly on Google for more information:

<https://nvd.nist.gov/vuln/detail/CVE-2024-27564>

<https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-27564>

<https://cybersecuritynews.com/chatgpt-vulnerability-actively-exploited/>