Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

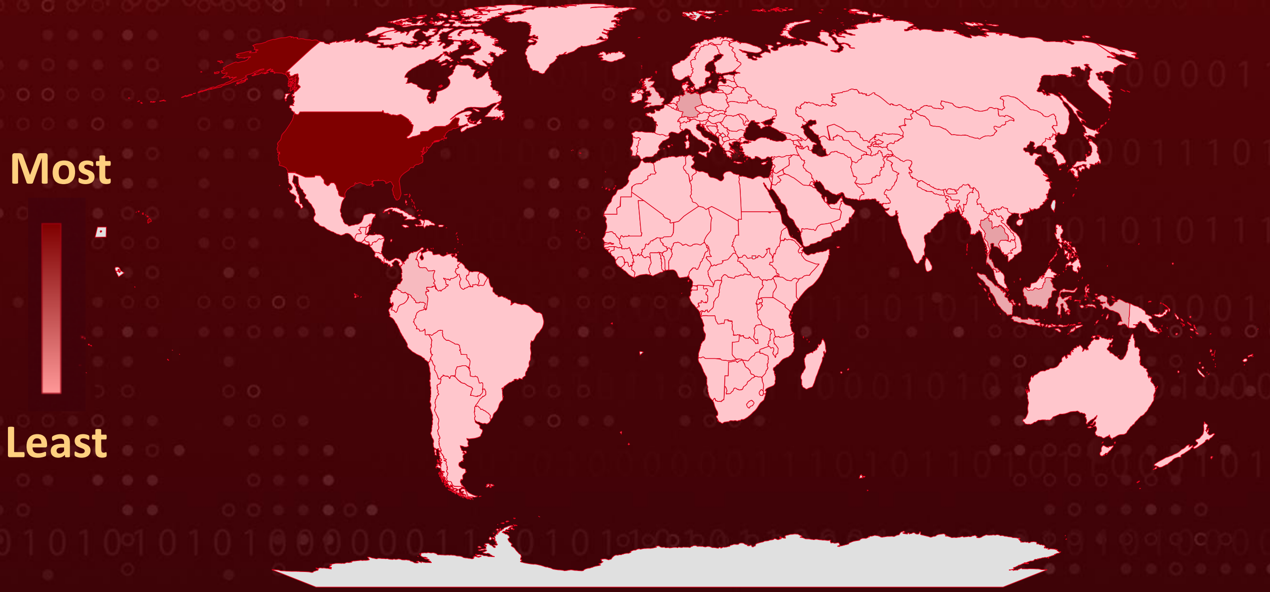
CVE-2024-27564: SSRF Vulnerability Puts AI-Integrated Systems at Risk

Date of Publication	Admiralty Code	TA Number
March 24, 2025	A1	TA2025092

Summary

First Seen: March 5, 2024
Affected Product: ChatGPT Pictureproxy.php
Targeted Industries: Finance, Government, and Healthcare
Impact: CVE-2024-27564 is an SSRF vulnerability in the pictureproxy.php component of certain ChatGPT implementations, allowing attackers to inject malicious URLs and force arbitrary requests. Despite its CVSS score of 6.5, it has been actively exploited, with over 10,479 attack attempts reported in a week. Key targets include financial, healthcare, and government sectors, with U.S. entities facing 33% of attacks. The EPSS score surged from 1.67% to 55.36%, highlighting the need for organizations to secure AI-integrated systems against exploitation.

Vulnerability Regions



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

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-27564	ChatGPT Pictureproxy.php Server-Side Request Forgery Vulnerability	ChatGPT Pictureproxy.php	✗	✗	✗

Vulnerability Details

#1 CVE-2024-27564 is a Server-Side Request Forgery (SSRF) vulnerability identified in the pictureproxy.php component of certain ChatGPT implementations(commit f9f4bbc), particularly in the dirk1983/mm1.ltd source code. This vulnerability stems from insufficient validation of the url parameter, allowing attackers to inject malicious URLs. Exploiting this flaw enables attackers to force the application to make arbitrary requests, potentially leading to unauthorized data access, internal network scanning, and further infiltration into sensitive systems.

#2 Despite its medium-severity classification with a CVSS score of 6.5, real-world exploitation has demonstrated its significant impact. The vulnerability was first published on March 5, 2024, and last updated on March 20, 2025. It has been actively exploited, with over 10,479 attack attempts reported globally within a single week. Multiple proof-of-concept (PoC) exploits are publicly available on platforms like GitHub, facilitating exploitation by attackers. The attacks have primarily targeted sectors such as finance, healthcare, and government organizations.

#3 Notably, U.S. government entities have faced 33% of these attacks, with other affected nations including Germany, Thailand, Indonesia, Colombia, and the United Kingdom. Additionally, the Exploit Prediction Scoring System (EPSS) score for this vulnerability surged from 1.67% to 55.36% following the wave of malicious activity.

#4 Research indicates that approximately 35% of organizations remain vulnerable due to misconfigurations in their Intrusion Prevention Systems (IPS), Web Application Firewalls (WAF), and firewall settings. Such misconfigurations leave systems exposed to exploitation and underscore the importance of robust security configurations.

#5 This situation highlights that vulnerability severity ratings do not always reflect real-world risks. Even a medium-severity vulnerability like CVE-2024-27564 can pose a significant threat when widely exploited. Organizations integrating AI technologies similar to ChatGPT must remain vigilant by continuously assessing their security configurations and promptly mitigating identified vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-27564	pictureproxy.php component (dirk1983/mm1.ltd, a third-party ChatGPT implementations)	cpe:2.3:a:dirk1983:chatgpt:2023-05-23:*:*:*:*:*:*:*	CWE-918

Recommendations

Patch and Update Affected Components: If you are using dirk1983/mm1.ltd or any similar ChatGPT-based implementation, check for security updates or patches from the vendor and apply them immediately.

Strengthen Input Validation and Sanitization: Implement strict validation and sanitization of user-supplied URLs in pictureproxy.php to prevent SSRF attacks.Use an allowlist approach for permitted URLs and reject external or untrusted requests. Encode user input properly and restrict URL parsing functions to avoid redirection-based exploits.

Implement Network Security Controls: Configure Web Application Firewalls (WAF) and Intrusion Prevention Systems (IPS) to detect and block SSRF attack patterns. Enforce firewall rules to prevent unauthorized outbound requests from server-side applications. Restrict direct internet access from internal services that do not require external communications.

Monitor and Detect Malicious Activity: Continuously monitor logs for unusual outbound requests originating from internal applications. Set up anomaly detection for unexpected network traffic patterns that could indicate SSRF exploitation.Utilize security information and event management (SIEM) solutions to detect and respond to threats in real-time.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0007 Discovery	T1588 Obtain Capabilities	T1588.005 Exploits	T1068 Exploitation for Privilege Escalation
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1203 Exploitation for Client Execution	T1083 File and Directory Discovery
T1133 External Remote Services	T1059 Command and Scripting Interpreter		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	31[.]56[.]56[.]156, 38[.]60[.]191[.]7, 94[.]156[.]177[.]106, 159[.]192[.]123[.]190, 119[.]82[.]255[.]34, 103[.]251[.]223[.]127, 104[.]143[.]229[.]115, 114[.]10[.]44[.]40, 116[.]212[.]150[.]192, 145[.]223[.]59[.]188, 167[.]100[.]106[.]99, 174[.]138[.]27[.]119, 212[.]237[.]124[.]38, 216[.]158[.]205[.]221

Patch Details

As of now, there is no official patch available for CVE-2024-27564. Organizations should implement strict input validation and access controls to mitigate this SSRF vulnerability.

References

https://veriti.ai/blog/veriti-research/cve-2024-27564-actively-exploited/

https://blackwellsecurity.com/resources/threat-bulletin/blackwell-helix-threat-bulletin-chatgpt-ssrf-vulnerability-cve-2024-27564-exploited-in-healthcare-attacks/

https://www.darkreading.com/cyberattacks-data-breaches/actively-exploited-chatgpt-bug-organizations-risk

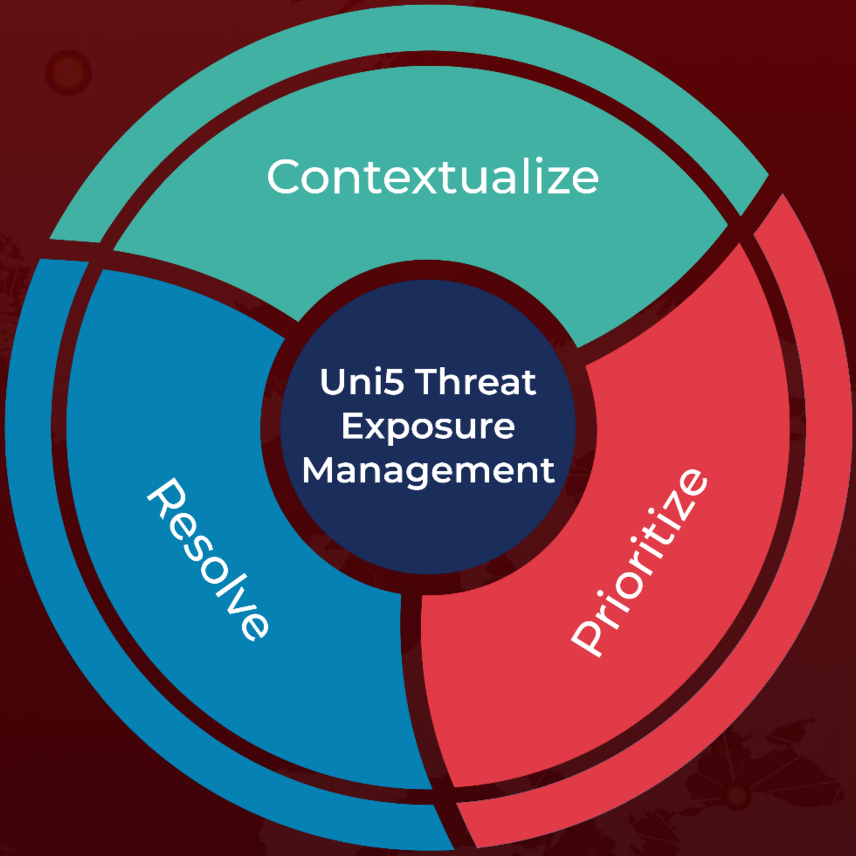
https://github.com/dirk1983/chatgpt/issues/114

https://www.broadcom.com/support/security-center/protection-bulletin/cve-2024-27564-chatgpt-commit-f9f4bbc-ssrf-vulnerability-exploited-in-the-wild

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

March 24, 2025 • 8:30 AM

More at www.hivepro.com