Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Aiohttp Vulnerability Leveraged by ShadowSyndicate

Date of Publication	Admiralty Code	TA Number
March 20, 2023	A1	TA2024107

Summary

First Seen: January 29, 2024
Affected Product: Aiohttp
Threat Actor: ShadowSyndicate
Impact: The cybercriminal group 'ShadowSyndicate' has been detected scanning for vulnerable servers, aiming to exploit a recently addressed vulnerability in the widely-used Aiohttp library. This exploit, if successful, could lead to unauthorized access to sensitive data on servers globally, posing a significant threat to organizations relying on Aiohttp for their web applications and services.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-23334	Aiohttp Directory Traversal Vulnerability	aiohttp: Prior to version 3.9.2	✗	✗	✓

Vulnerability Details

#1 The cybercriminal group 'ShadowSyndicate' has been detected engaging in scans for servers susceptible to CVE-2024-23334, aiming to exploit a recently addressed vulnerability in Aiohttp. This exploit has the potential to impact numerous servers globally. The security loophole involves a directory traversal flaw within aiohttp, enabling unauthorized remote attackers to retrieve sensitive data from arbitrary files on the server if successfully exploited.

#2 Aiohttp, an open-source library integrated with Python's asynchronous I/O framework, Asyncio, is designed to manage vast numbers of concurrent HTTP requests without relying on conventional thread-based networking. It serves as a crucial tool for tech firms, web developers, backend engineers, and data scientists seeking to construct high-performance web applications and services that consolidate data from various external APIs.

#3 An estimated 70,000 internet-accessible aiohttp instances are distributed worldwide, with significant concentrations in the United States, China, Germany, Thailand, and the United Kingdom. Unfortunately, determining the specific versions of these instances is challenging, complicating efforts to gauge the extent of vulnerability among aiohttp servers. The scanning activities conducted by the ShadowSyndicate group underscore the imminent danger posed by this security threat.

#4 ShadowSyndicate recognized as an opportunistic and financially-driven threat entity, has been active since July 2022 and has been tentatively associated with ransomware strains such as Quantum, Nokoyawa, BlackCat/ALPHV, Clop, Royal, Cactus, and Play. The prolonged use of outdated versions of open-source libraries, often due to practical challenges in locating and implementing patches, renders them valuable targets for threat actors. Consequently, even years after security updates have been released, these libraries remain susceptible to exploitation in cyberattacks.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-23334	aiohttp: 1.0.5 - 3.9.1	cpe:2.3:a:aiohttp:aiohttp:*:*:*:*:*:*:*:*	CWE-22

Recommendations

Apply Official Fixes Immediately: While upgrading to a patched version of Aiohttp is crucial, it's advisable to implement additional security measures regardless. This ensures comprehensive protection against potential vulnerabilities.

Disable follow_symlinks=True: If the follow_symlinks=True option is utilized outside of a restricted local development environment, it should be disabled immediately. This option poses a significant risk, even after the CVE has been addressed. It's unnecessary for following symlinks within the static root directory and should only be used cautiously to prevent symlink exploitation.

Utilize Reverse Proxy Server: Aiohttp users are strongly advised to employ a reverse proxy server, such as nginx, to manage static resources instead of relying on Aiohttp for production environments. This practice not only safeguards against the identified vulnerability but also reduces the likelihood of exploitation.

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

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0042 Resource Development	TA0007 Discovery	TA0003 Persistence
TA0010 Exfiltration	T1059 Command and Scripting Interpreter	T1543 Create or Modify System Process	T1588 Obtain Capabilities
T1082 System Information Discovery	T1588.002 Tool	T1587.004 Exploits	T1567 Exfiltration Over Web Service
T1083 File and Directory Discovery			

Indicator of Compromise (IOCs)

TYPE	VALUE
IPv4	81[.]19[.]136[.]251, 157[.]230[.]143[.]100, 170[.]64[.]174[.]95, 103[.]151[.]172[.]28, 143[.]244[.]188[.]172

Patch Details

Upgrade to a patched version 3.9.2 of aiohttp

Link:
https://github.com/aio-libs/aiohttp/security/advisories/GHSA-5h86-8mv2-jq9f

References

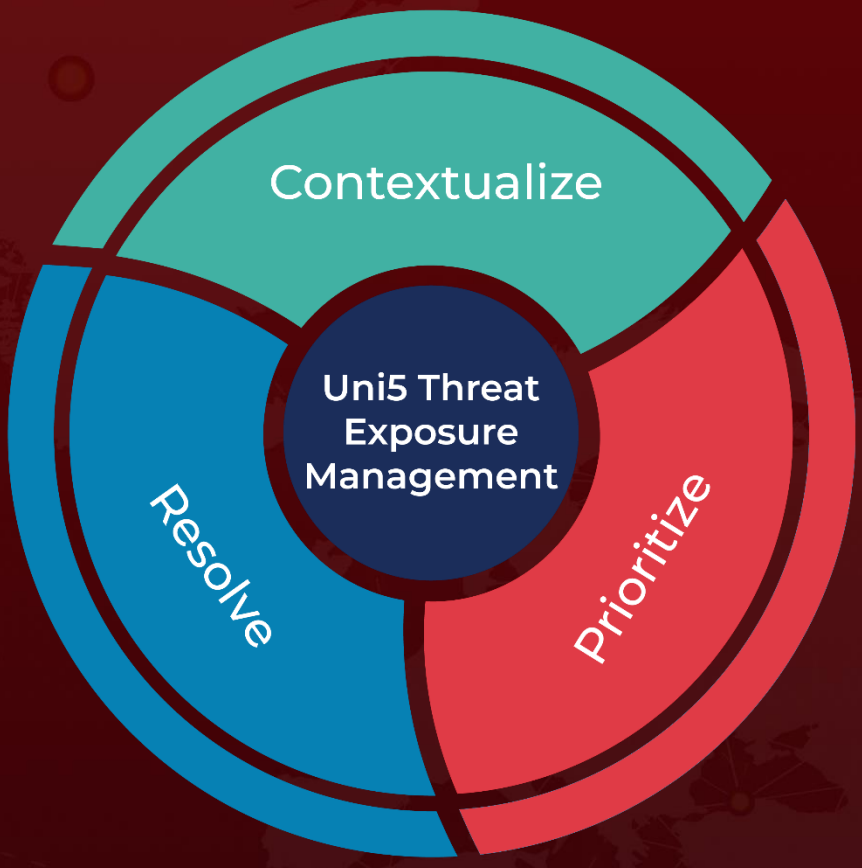
https://cyble.com/blog/cgsi-probes-shadowsyndicate-groups-possible-exploitation-of-aiohttp-vulnerability-cve-2024-23334/

https://gist.github.com/W01fh4cker/2b570b1d0df40aa94808184c231d7ecb

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 20, 2024 • 4:00 AM

More at www.hivepro.com