

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Tinyproxy Vulnerability Exposes Hosts to Remote Code Execution

Date of Publication

May 7, 2024

Last Update Date

May 14, 2024

Admiralty Code

A1

TA Number

TA2024174




Summary

Discovered: December 2023

Affected Products: Tinyproxy

Impact: CVE-2023-49606 a critical use-after-free vulnerability found in Tinyproxy's HTTP Connection Headers parsing feature. This flaw can be exploited by utilizing a meticulously crafted HTTP header, triggering the reutilization of previously freed memory. Consequently, this misuse leads to memory corruption, posing a significant risk of remote code execution.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-49606	Tinyproxy HTTP Connection Headers Use-After-Free Vulnerability	Tinyproxy			

Vulnerability Details

#1 CVE-2023-49606 is a severe security flaw discovered in the Tinyproxy HTTP/HTTPS proxy tool, with a CVSS score of 9.8. This critical vulnerability affects versions 1.10.0 and 1.11.1, presenting a use-after-free bug. If exploited, this flaw can lead to memory corruption and potentially allow remote code execution.

#2 This vulnerability allows a remote attacker to compromise a system by exploiting a use-after-free error in the HTTP Connection Headers parsing mechanism. By sending a specially crafted HTTP header, the attacker can execute arbitrary code on the targeted system.

#3

Tinyproxy is a lightweight and open-source HTTP proxy daemon known for its simplicity and efficiency. As of May 2024, there are approximately 90,000+ hosts publicly exposing a Tinyproxy service. Alarming, about 57% hosts are running vulnerable versions. These exposed hosts are mainly located in the United States, South Korea, China, France, and Germany.

#4

To mitigate the risk, users are strongly urged to update to the latest version 1.11.2 of Tinyproxy. Additionally, it's advisable to limit the exposure of the Tinyproxy service to the public internet wherever feasible.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-49606	Tinyproxy 1.11.1 and Tinyproxy 1.10.0	cpe:2.3:a:tinyproxy:tinyproxy:1.10.0:*:*:*:*:* cpe:2.3:a:tinyproxy:tinyproxy:1.11.1:*:*:*:*:*	CWE-416

Recommendations



Update: The fixed version of the software is now available. Organizations can take proactive measures to update to the latest version 1.11.2 of Tinyproxy.



Block Rogue HTTP Requests: Implement a proactive rule in the Web Application Firewall to scrutinize and intercept suspicious HTTP requests carrying rogue headers. Identify and thwart such requests structured as {HTTP Header}: {HTTP Header}, as they could be indicative of attempts to exploit vulnerabilities.



Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>T1588</u> Obtain Capabilities
<u>T1588.006</u> Vulnerabilities	<u>T1059</u> Command and Scripting Interpreter	<u>T1190</u> Exploit Public-Facing Application	

Patch Details

The fixed version is now available, organizations can update to the latest version 1.11.2 of Tinyproxy.

Link: <https://github.com/tinyproxy/tinyproxy/releases/tag/1.11.2>

References

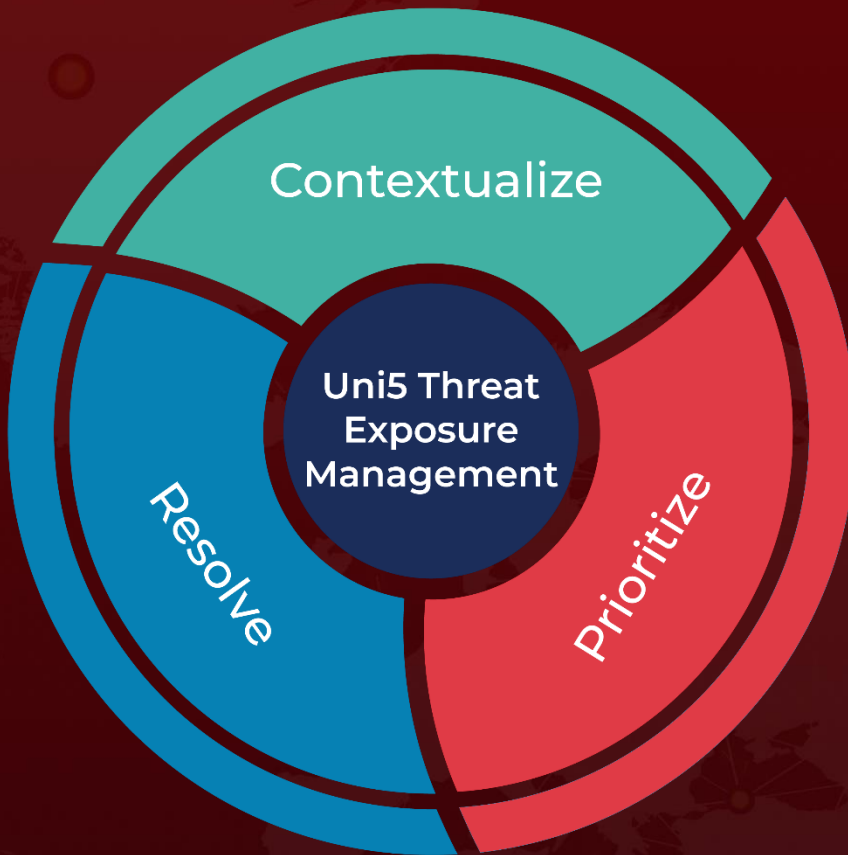
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1889

<https://github.com/tinyproxy/tinyproxy/issues/533>

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

May 7, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com