



Threat Level

 **Amber**

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Critical Remote Code Execution Vulnerabilities Discovered in ASUS Routers

Date of Publication

September 8, 2023

Admiralty Code

A1

TA Number

TA2023361










Summary

First Seen: September 5, 2023

Affected Product: ASUS RT-AX55, RT-AX56U_V2, and RT-AC86U routers

Impact: Three critical-severity remote code execution vulnerabilities have been identified in ASUS routers. These vulnerabilities have the potential to allow threat actors to take control of these devices if the required security updates have not been applied.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-39238	ASUS Format String Vulnerability	ASUS RT-AX55, RT-AX56U_V2, RT-AC86U			
CVE-2023-39239	ASUS Format String Vulnerability	ASUS RT-AX55, RT-AX56U_V2, RT-AC86U			
CVE-2023-39240	ASUS Format String Vulnerability	ASUS RT-AX55, RT-AX56U_V2, RT-AC86U			

Vulnerability Details

#1

ASUS routers, RT-AX55, RT-AX56U_V2, and RT-AC86U models, have been found to be affected by three critical remote code execution vulnerabilities. These vulnerabilities pose a significant risk, as they could potentially enable threat actors to gain unauthorized access and take control of the affected devices.

#2

The three vulnerabilities, CVE-2023-39238, CVE-2023-39239, and CVE-2023-39240, are categorized as format string vulnerabilities. These vulnerabilities have the concerning characteristic of being remotely exploitable without requiring authentication. Exploiting these vulnerabilities could lead to severe consequences, including remote code execution, service disruptions, and the ability to carry out arbitrary operations on the affected device.

#3

The CVE-2023-39238 vulnerability is attributed to a lack of proper input format string verification within the `set_iperf3_svr.cgi` module. The CVE-2023-39239 vulnerability involves a format string vulnerability within the API of the general setting function. The CVE-2023-39240 vulnerability arises due to a lack of proper verification of the input format string in the iperf-related API module. The remote attackers can exploit these vulnerabilities without requiring any permissions.

#4

ASUS has released patches to address these vulnerabilities in their routers. By applying these patches and keeping their systems up to date, users can enhance the security of their devices, safeguarding them from potential remote attacks by malicious actors.

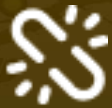
Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-39238	RT-AX55: 3.0.0.4.386_50460 RT-AX56U_V2: 3.0.0.4.386_50460 RT-AC86U: 3.0.0.4_386_51529	cpe:2.3:h:asus:rt-ax55:3.0.0.4.386_50460:*:*:*:*:*	CWE-134
CVE-2023-39239	RT-AX55: 3.0.0.4.386_50460 RT-AX56U_V2: 3.0.0.4.386_50460 RT-AC86U: 3.0.0.4_386_51529	cpe:2.3:h:asus:rt-ax55:3.0.0.4.386_50460:*:*:*:*:*	CWE-134
CVE-2023-39240	RT-AX55: 3.0.0.4.386_50460 RT-AX56U_V2: 3.0.0.4.386_50460 RT-AC86U: 3.0.0.4_386_51529	cpe:2.3:h:asus:rt-ax55:3.0.0.4.386_50460:*:*:*:*:*	CWE-134

Recommendations



Apply Patch: Install the security patch provided by ASUS to address the CVE-2023-39238, CVE-2023-39239, CVE-2023-39240 vulnerabilities. This patch closes the security gap that allows attackers to exploit the unauthenticated remote code execution vulnerability.



Access Control: Disabling remote administration (WAN Web Access) on your ASUS router is an important step to enhance security and prevent unauthorized access from the internet.



Detection Tools: Employing monitoring and alerting systems is an excellent practice for enhancing the security of your network and promptly detecting unusual or unauthorized access activities.

Potential MITRE ATT&CK TTPs

<u>TA0040</u> Impact	<u>TA0002</u> Execution	<u>TA0006</u> Credential Access	<u>T1496</u> Resource Hijacking
<u>T1106</u> Native API	<u>T1190</u> Exploit Public-Facing Application	<u>T1556</u> Modify Authentication Process	<u>T1556.004</u> Network Device Authentication

Patch Details

Apply the Following Firmware Updates:

RT-AX55: 3.0.0.4.386_51948 or later

RT-AX56U_V2: 3.0.0.4.386_51948 or later

RT-AC86U: 3.0.0.4.386_51915 or later

Links:

https://www.asus.com/networking-iot-servers/wifi-routers/all-series/rt-ax55/helpdesk_bios/?model2Name=RT-AX55

https://www.asus.com/supportonly/rt-ac86u/helpdesk_bios/?model2Name=RT-AC86U

References

https://securityaffairs.com/150399/iot/asus-routers-critical-rces.html?web_view=true

<https://www.twcert.org.tw/tw/cp-132-7354-4e654-1.html>

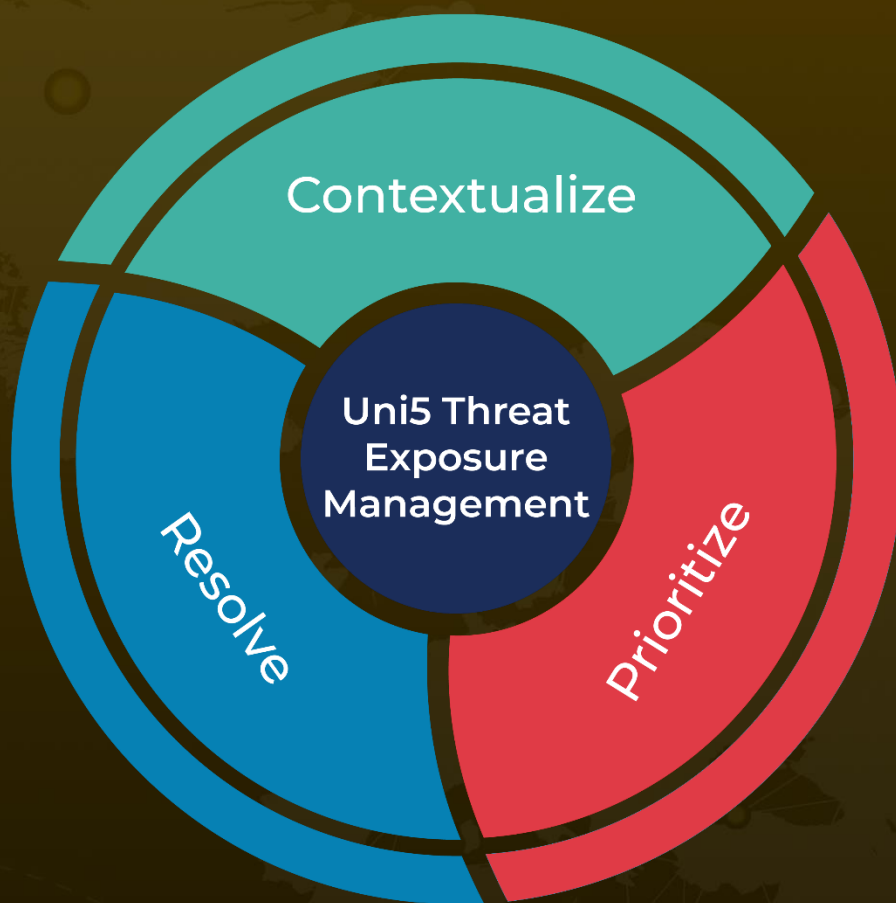
<https://www.twcert.org.tw/tw/cp-132-7355-0ce8d-1.html>

<https://www.twcert.org.tw/tw/cp-132-7356-021bf-1.html>

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

September 8, 2023 • 6:40 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com