Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

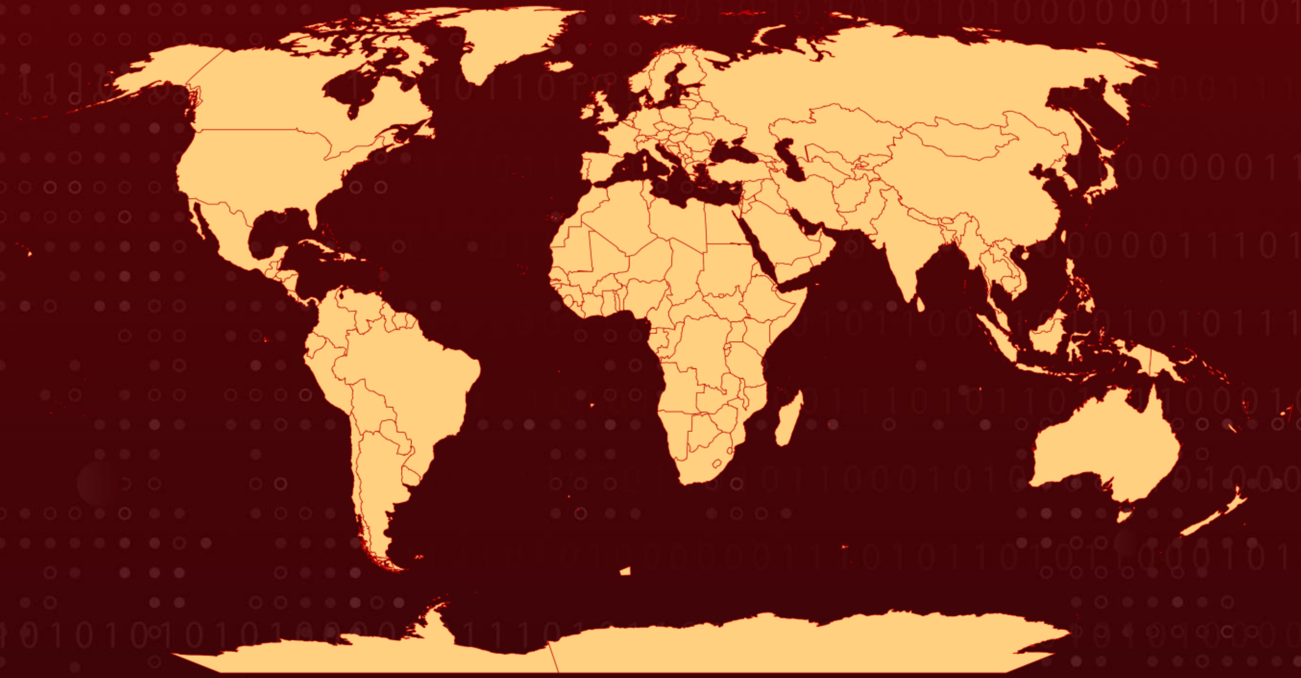
New AndoryuBot Malware Exploits Ruckus Wireless Flaw for DDoS Attacks

Date of Publication	Admiralty Code	TA Number
May 10, 2023	A1	TA2023219

Summary

First Seen: February 2023
Targeted Countries: Worldwide
Affected Platform: Linux
Malware: AndoryuBot
Attack: AndoryuBot targets critical Ruckus Wireless Admin panel vulnerability to infect Wi-Fi access points for use in DDoS attacks, malware supports 12 DDoS attack modes and is marketed through YouTube videos.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA	PATCH
CVE-2023-25717	Ruckus Remote Code Execution Vulnerability	All Ruckus Wireless Admin panels version 10.4 and older	✗	✓	✓

Attack Details

#1

A new botnet named AndoryuBot was found exploiting a critical vulnerability in Ruckus wireless Access Point (AP) devices. The vulnerability affects all Ruckus Wireless Admin panels version 10.4 and older. The botnet aims to enlist vulnerable devices to its DDoS swarm, which it operates for profit.

#2

The botnet utilizes a DDoS attack module for various protocols and communicates with its command-and-control server using SOCKS5 proxies. Once AndoryuBot gains access to a device, it downloads a script for further propagation. The malware targets multiple architectures and communicates with the server using a hardcoded User-Agent string.

#3

The AndoryuBot malware supports 12 DDoS attack modes and is currently marketed through YouTube videos. The botnet first appeared in February 2023, and it was observed in April 2023.

Recommendations

Apply available firmware updates: If you are using Ruckus Wireless devices, make sure to apply the available security updates that address the vulnerability (CVE-2023-25717) that the AndoryuBot malware exploits. If your device has reached end-of-life and is no longer receiving updates, consider upgrading to a newer model that is still supported.

Use strong passwords: Ensure that you are using strong, unique passwords for device administrator accounts. Avoid using default or easily guessable passwords, and consider implementing multi-factor authentication (MFA) to add an extra layer of protection.

Disable remote admin panel access: If remote admin panel access is not needed for your device, disable it to prevent potential attacks that exploit vulnerabilities in remote access protocols.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0011 Command and Control	TA0002 Execution	TA0040 Impact
TA0003 Persistence	TA0001 Initial Access	TA0042 Resource Development	T1190 Exploit Public-Facing Application
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	T1140 Deobfuscate/Decode Files or Information
T1203 Exploitation for Client Execution	T1584 Compromise Infrastructure	T1090 Proxy	T1090.002 External Proxy
T1584.005 Botnet	T1499 Endpoint Denial of Service	T1204 User Execution	T1204.002 Malicious File

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	163[.]123[.]142[.]146 45[.]153[.]243[.]39
SHA256	ea064dd91d8d9e6036e99f5348e078c43f99fdf98500614bffb736c4b0fff408 f42c6cea4c47bf0cbef666a8052633ab85ab6ac5b99b7e31faa1e198c4dd1ee1 3441e88c80e82b933bb09e660d229d74f7b753a188700fe018e74c2db7b2aaa0 3c9998b8451022beee346f1afe18cab84e867b43c14ba9c7f04e5c559bfc4c3a b71b4f478479505f1bfb43663b4a4666ec98cd324acb16892ecb876ade5ca6f9 e740a0d2e42c09e912c43ecdc4dcbd8e92896ac3f725830d16aaa3eddf07fd5c 4fe4cff875ef7f8c29c95efe71b92ed31ed9f61eb8dfad448259295bd1080aca 2e7136f760f04b1ed7033251a14fef1be1e82ddcbff44dae30db12fe52e0a78a 1298da097b1c5bdce63f580e14e2c1b372c409476747356a8e9cfaf62b94513d 55e921a196c92c659305aa9de3edf6297803b60012f83967562a57547875fec1

Patch Links

https://support.ruckuswireless.com/security_bulletins/315

References

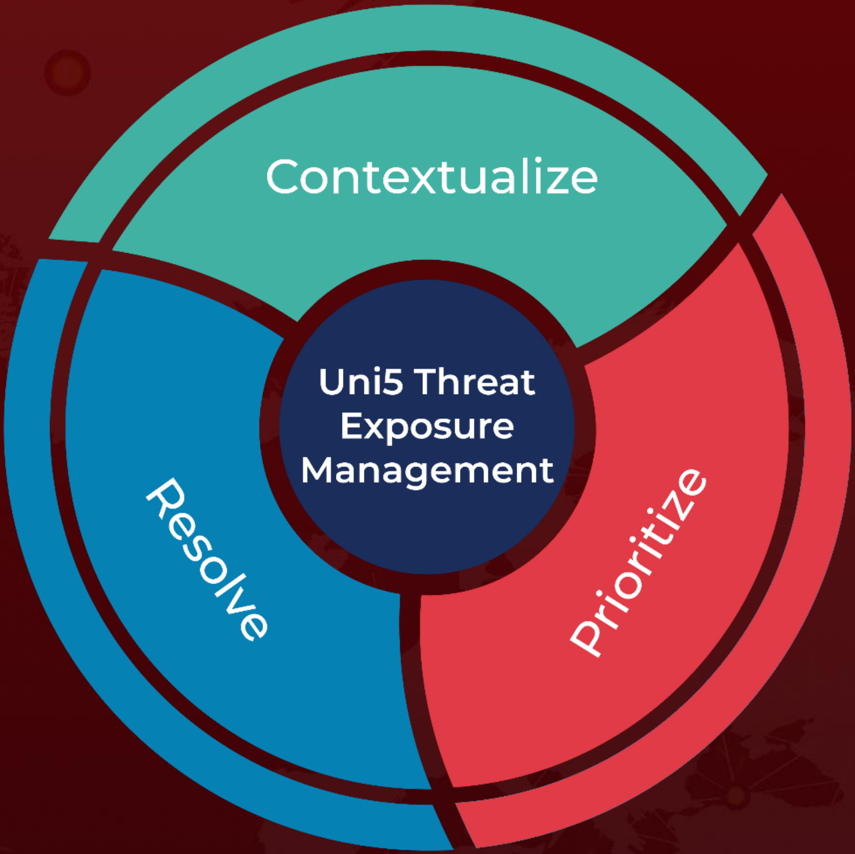
https://www.fortinet.com/blog/threat-research/andoryubot-new-botnet-campaign-targets-ruckus-wireless-admin-remote-code-execution-vulnerability-cve-2023-25717

https://www.cisa.gov/news-events/alerts/2023/05/12/cisa-adds-seven-known-exploited-vulnerabilities-catalog

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 10, 2023 • 04:30 AM

More at www.hivepro.com