Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

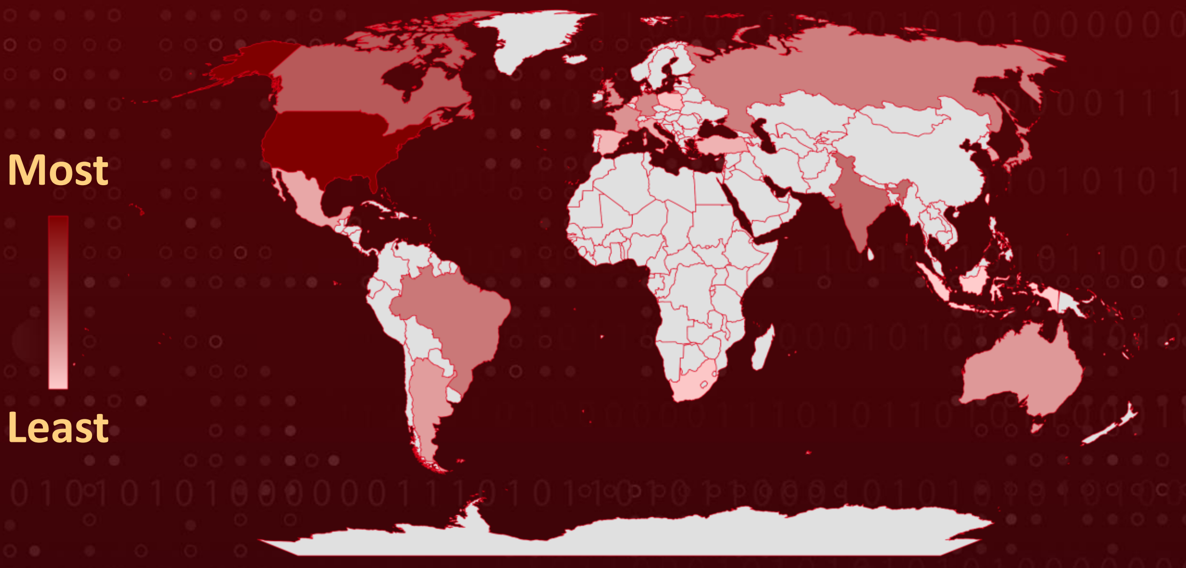
PolarEdge Botnet Turns Edge Devices Into Cyber Weapons

Date of Publication	Admiralty Code	TA Number
March 11, 2025	A1	TA2025071

Summary

Active Since: Late 2023
Malware: PolarEdge Botnet
Top Targeted Countries: United States, Canada, India, Brazil, Russia, Japan, Germany, United Kingdom, France, Australia, Argentina, South Korea, Mexico, Italy, Turkey, Spain, Netherlands, Poland, South Africa, Indonesia, Taiwan
Targeted Devices: Cisco, ASUS, QNAP, Synology
Attack: A silent cyber threat is creeping through the internet, hijacking routers from Cisco, ASUS, QNAP, and Synology into a covert botnet known as PolarEdge. Exploiting a hidden flaw, attackers plant an undetectable backdoor, turning everyday devices into unwitting accomplices for cyber warfare. With over 2,000 infected systems worldwide and an infrastructure built for stealth, this operation has been lurking in the shadows since late 2023 its true purpose is still unknown.

Attack 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-2023-20118	Cisco Small Business RV Series Routers Command Injection Vulnerability	Cisco Small Business RV Series Routers	✗	✓	EOL

Attack Details

#1

A newly identified malware campaign is actively targeting edge devices from Cisco, ASUS, QNAP, and Synology, enlisting them into a botnet known as PolarEdge. The attackers exploit CVE-2023-20118, a vulnerability that enables remote command execution (RCE). By leveraging this flaw, they deploy a web shell onto compromised routers, ultimately infecting them with an undocumented implant.

#2

This implant reveals that it functions as a TLS backdoor, equipped with predefined commands to facilitate remote control. Additional payloads targeting different device manufacturers led to the discovery of a botnet comprising over 2,000 infected assets worldwide. This network, operational since at least late 2023, is now linked to a broader malicious infrastructure.

#3

At the heart of the attack is the exploitation of the *delete_cert* function, which constructs and executes a *rm* command based on user input. Due to insufficient validation, attackers can inject arbitrary commands using specially crafted inputs, leading to full system compromise. The vulnerability arises from improper concatenation of user-supplied data into system calls without sanitization, making it susceptible to command injection.

#4

The infection chain typically begins with the execution of a shell script named "q", which downloads, installs, and executes the payload on a breached system. Once active, PolarEdge enters an infinite loop, establishing a TLS session and spawning a child process to manage client connections and execute commands via *exec_command*.

#5

Given its capabilities, one plausible objective of PolarEdge is to convert compromised devices into Operational Relay Boxes (ORBs) strategic footholds used to launch offensive cyber operations. The PolarEdge botnet's reach extends across multiple regions, with the majority of infections observed in the United States, Taiwan, Russia, India, Brazil, Australia, and Argentina. As this campaign continues to evolve, its scale and impact raise significant cybersecurity concerns.

Recommendations

Disable Remote Management & Restrict Port Access: To mitigate the PolarEdge botnet threat, administrators should disable remote management by accessing the device's web-based interface, navigating to Firewall > General, and unchecking the Remote Management option. Blocking ports 443 and 60443 is also essential this can be done by creating access rules in Firewall > Access Rules to deny traffic on these ports. Additionally, keeping firmware updated, enforcing strong credentials and MFA, disabling unused services like Telnet and UPnP, and implementing network segmentation can significantly reduce attack risks.

Replace End-of-Life Equipment: Upgrade and replace devices that have reached their end-of-life status and are no longer supported by their vendors. Utilizing devices under active support plans ensures that they receive necessary security updates and patches, reducing vulnerabilities.

Network Segmentation & Zero Trust Implementation: Segment critical infrastructure to isolate sensitive data and limit lateral movement. Implement Zero Trust Network Access (ZTNA) by enforcing identity-based policies rather than traditional perimeter security.

Device Attestation & Hardware Security: To mitigate the PolarEdge botnet threat, organizations should implement device attestation to ensure that only trusted, uncompromised devices can connect to the network. This prevents attackers from using hijacked edge devices as entry points. Additionally, deploying hardware security modules (HSMs) can protect cryptographic keys from being exfiltrated or manipulated by malware, reducing the risk of unauthorized control over compromised devices.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0040** Impact	**T1057** Process Discovery	**T1082** System Information Discovery

T1083 File and Directory Discovery	T1046 Network Service Discovery	T1027 Obfuscated Files or Information	T1027.013 Encrypted/Encoded File
T1190 Exploit Public-Facing Application	T1133 External Remote Services	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell
T1543 Create or Modify System Process	T1505 Server Software Component	T1505.003 Web Shell	T1055 Process Injection
T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1562.002 Disable Windows Event Logging	T1562.003 Impair Command History Logging
T1070.001 Clear Windows Event Logs	T1070 Indicator Removal	T1070.004 File Deletion	T1070.009 Clear Persistence

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13, 464f29d5f496b4acffc455330f00adb34ab920c66ca1908eee262339d6946bcd, 932b2545bd6e3ad74b82ca2199944edecf9c92ad3f75fce0d07e04ab084824d5, 121969d72f8e6f09ad93cf17500c479c452e230e27e7b157d5c9336dff15b6ef, 1ca7262f91d517853a0551b14abb0306c4e3567e41b1e82a018f0aac718e499e, eda7cc5e1781c681afe99bf513fcaf5ae86afbf1d84dfd23aa563b1a043cbba8
URL	hxxps[:]//asustordownload[.]com[:]45674, hxxps[:]//siotherlentsearsitech[.]shop[:]58425, hxxps[:]//122[.]8[.]183[.]181[:]59711, hxxps[:]//ssofhoseuegsgrfnu[.]ru/inet_pton
IPv4	195[.]123[.]212[.]54, 119[.]8[.]186[.]227, 43[.]129[.]205[.]244, 122[.]8[.]183[.]181, 159[.]138[.]119[.]99

TYPE	VALUE
Domains	longlog[.]cc, landim[.]cc, hitchil[.]cc, logchim[.]cc, aipricadd[.]top, firebasesafer[.]top, largeroofs[.]top, gardensc[.]cc, headached[.]cc, durianlink[.]cc, nternetd[.]cc, suiteiol[.]cc, centrequ[.]cc, icecreand[.]cc, ssofhoseuegsgrfnu[.]ru, siotherlentsearsitech[.]shop, asustordownload[.]com

Patch Details

Cisco has neither released nor planned any software updates to remediate the CVE-2023-20118 vulnerability detailed in this advisory. The Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 routers have reached the ***end-of-life*** stage and will ***no longer receive official support or security patches.***

Link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5

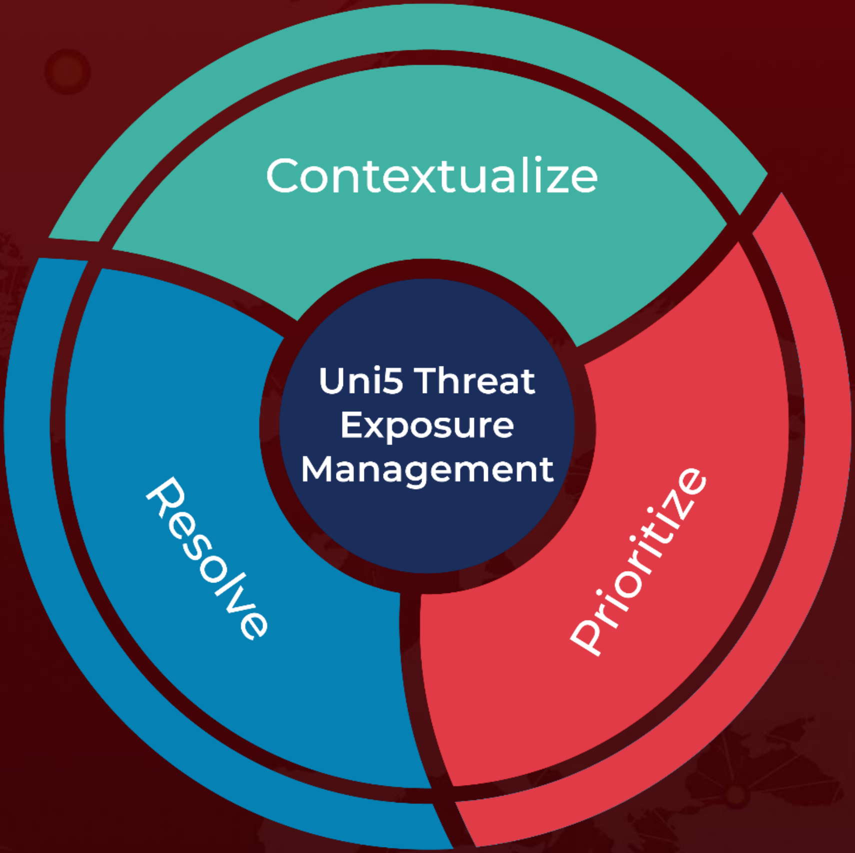
References

https://blog.sekoia.io/polaredge-unveiling-an-uncovered-iot-botnet/

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 11, 2025 • 5:30 AM

More at www.hivepro.com