Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

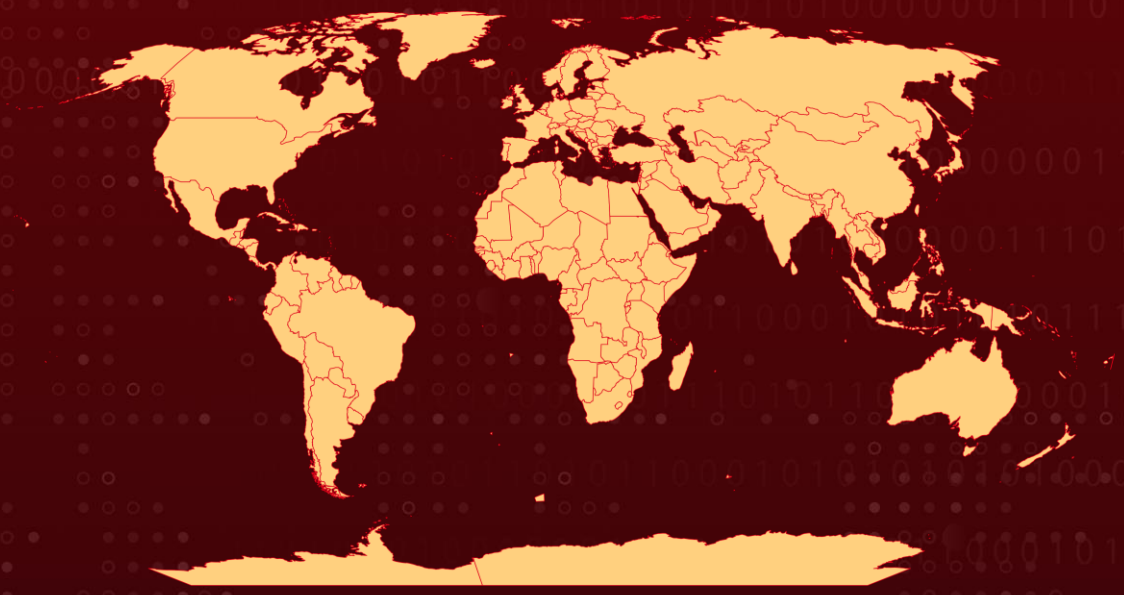
Mirai Botnet's Offspring InfectedSlurs Exploits Dual Zero-Days

Date of Publication	Last Update Date	Admiralty Code	TA Number
November 24, 2023	January 2, 2024	A1	TA2023476

Summary

Attack Began: October 2023
Malware: InfectedSlurs, JenX Mirai
Attack Region: Worldwide
Affected Products: QNAP VioStor NVR, FXC AE1021, AE1021PE
Attack: A new Mirai-based malware botnet, InfectedSlurs, is actively conducting a sophisticated campaign by exploiting two zero-day remote code execution (RCE) vulnerabilities in routers and video recorder (NVR) devices. These vulnerabilities, currently being exploited in the wild, facilitate the creation of a distributed denial-of-service (DDoS) botnet.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-49897	FXC OS command injection vulnerability	FXC AE1021 & AE1021PE version 2.0.9 and earlier	✓	✓	✓
CVE-2023-47565	QNAP VioStor OS command injection vulnerability	QVR Firmware 4.x	✓	✓	✓

Attack Details

#1 A recently discovered malware botnet named 'InfectedSlurs' is actively conducting a sophisticated campaign, leveraging two zero-day remote code execution (RCE) vulnerabilities to compromise routers and video recorder (NVR) devices. These vulnerabilities, currently being exploited in the wild, serve as channels for establishing a distributed denial-of-service (DDoS) botnet.

#2 The malware seizes control of infected devices, incorporating them into its DDoS swarm, presumably for lucrative rental purposes. InfectedSlurs first emerged in late October 2023, with details of the vulnerabilities deliberately withheld to provide implicated vendors an opportunity to release patches and preempt potential exploitation by other malicious entities.

#3 The campaign began with initial low-frequency probes utilizing authentication via POST requests, followed by a subsequent command injection attempt. The threat actor exploits RCE flaws in QNAP VioStor and FXC firmware to gain authenticated access by modifying the device's NTP settings.

#4 The botnet's command-and-control (C2) servers and hard-coded strings align with a JenX Mirai malware variant revealed in January 2018. The C2 infrastructure demonstrates concentration and appears to support hailBot operations. Significantly, the attack mechanisms closely resemble those of the original Mirai botnet. Like Mirai, InfectedSlurs lacks a persistence mechanism. A temporary disruption of the botnet can be achieved by rebooting NVR and router devices.

Recommendations

Apply Official Fixes Immediately: For optimal security, it is strongly advised to promptly implement the following official fixes: update the FXC firmware to version 2.0.10, perform a factory reset, and modify the default password. Additionally, QNAP recommends that users download and apply the latest QVR Firmware, as both QVR Firmware 5.x and 4.x have reached end-of-life status according to QNAP's official statement.

Temporary Disruption Measures: Consider implementing temporary disruption measures for the affected devices. Rebooting NVR and router devices, as suggested, can serve as a short-term preventive measure until a patch is applied.

Continuous Monitoring of C2 Infrastructure: Given the concentration of InfectedSlurs' command-and-control (C2) servers, organizations should continuously monitor and block connections to these servers. This proactive approach can disrupt the botnet's communication channels and limit its effectiveness.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

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

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control
TA0040 Impact	T1059 Command and Scripting Interpreter	T1203 Exploitation for Client Execution	T1659 Content Injection
T1583.005 Botnet	T1588.006 Vulnerabilities	T1543 Create or Modify System Process	T1574 Hijack Execution Flow
T1046 Network Service Discovery	T1105 Ingress Tool Transfer	T1499 Endpoint Denial of Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	infectedchink[.]cat, opewu[.]homes, wu[.]qwewu[.]site, dfvzfvd[.]help, husd8uasd9[.]online, homehitter[.]tk, shetoldmeshewas12[.]oss, shetoldmeshewas12[.]geek, shetoldmeshewas12[.]pirate, shetoldmeshewas12[.]dyn, shetoldmeshewas12[.]libre, shetoldmeshewas12[.]gopher, shetoldmeshewas12[.]parody, shetoldmeshewas13[.]oss, shetoldmeshewas13[.]geek, shetoldmeshewas13[.]pirate, shetoldmeshewas13[.]dyn, shetoldmeshewas13[.]libre, shetoldmeshewas13[.]gopher, shetoldmeshewas13[.]parody, hujunxa[.]cc, skid[.]uno, dogeating[.]monster, chinkona[.]buzz, dogeatingchink[.]uno, infectedchink[.]cat, infectedchink[.]online, sdfsd[.]xyz, gottalovethe[.]indy, pqahzam[.]ink, cooldockmantoo[.]men, chinks-eat-dogs[.]africa, cnc[.]kintaro[.]cc, fuckmy[.]site, fuckmy[.]store, hbakun[.]geek, ksarpo[.]parody, rwziag[.]pirate, metbez[.]gopher, rmdtqq[.]libre,

TYPE	VALUE
Domains	pektbo[.]libre, mqcgbs[.]gopher, cbdgzy[.]pirate, czbrwa[.]geek, edrnhe[.]oss, hfoddy[.]dyn, fawzpp[.]indy, hxqytk[.]geek, iaxtpa[.]parody, mfszki[.]gopher, qhedye[.]oss, wnisyi[.]libre, asdjjasdhioasdia[.]online, jiggaboojones[.]tech
SHA256	dabdd4b5a3a70c64c031126fad36a4c45feb69a45e1028d79da6b443291addb8, 3f3c2e779f8e3d7f2cc81536ef72d96dd1c7b7691b6e613f5f76c3d02909edd8, 75ef686859010d6164bcd6a4d6cf8a590754ccc3ea45c47ace420b02649ec380, f8abf9fb17f59cbd7381aa9f5f2e1952628897cee368defd6baa6885d74f3ecc, 8777f9af3564b109b43cbcf1fd1a24180f5cf424965050594ce73d754a4e1099, ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1, a4975366f0c5b5b52fb371ff2cb034006955b3e3ae064e5700cc5365f27a1d26, cd93264637cd3bf19b706afc19944dfb88cd27969aaf0077559e56842d9a0f87, 8e64de3ac6818b4271d3de5d8e4a5d166d13d12804da01ce1cdb7510d8922cc6, 35fcc2058ae3a0af68c5ed7452e57ff286abe6ded68bf59078abd9e7b11ea90a, 7cc62a1bb2db82e76183eb06e4ca84e07a78cfb71241f21212afd1e01cb308b2, 29f11b5d4dbd6d06d4906b9035f5787e16f9e23134a2cc43dfc1165127c89bff, cfbcbb876064c2cf671bdae61544649fa13debbbe58b72cf8c630b5bfc0649f9, a3b78818bbef4fd55f704c96c203765b5ab37723bc87aac6aa7ebfcc76dfa06d, ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1
IPv4	45.142.182[.]96

Patch Details

Update the FXC firmware to 2.0.10, perform a factory reset, and change the default password.

Link:
https://www.fxc.jp/form/certify/

Update the QVR Firmware to 5.x and later

Link:
https://www.qnap.com/en/download

References

https://www.akamai.com/blog/security-research/new-rce-botnet-spreads-mirai-via-zero-days

https://www.fxc.jp/news/20231206

https://www.qnap.com/en/security-advisory/qsa-23-48

https://www.cisa.gov/news-events/ics-advisories/icsa-23-355-02

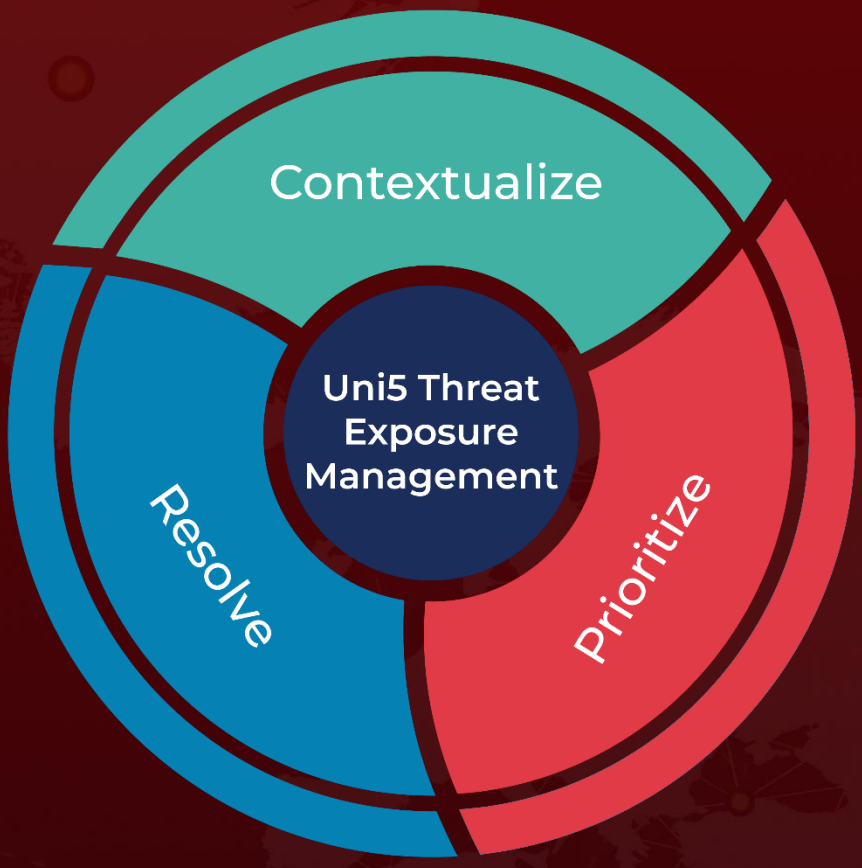
https://www.cisa.gov/news-events/ics-advisories/icsa-23-355-01

https://www.hivepro.com/threat-advisory/deciphering-mirais-next-chapter-the-strategies-of-the-latest-players/

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

November 24, 2023 . 5:30 AM

More at www.hivepro.com