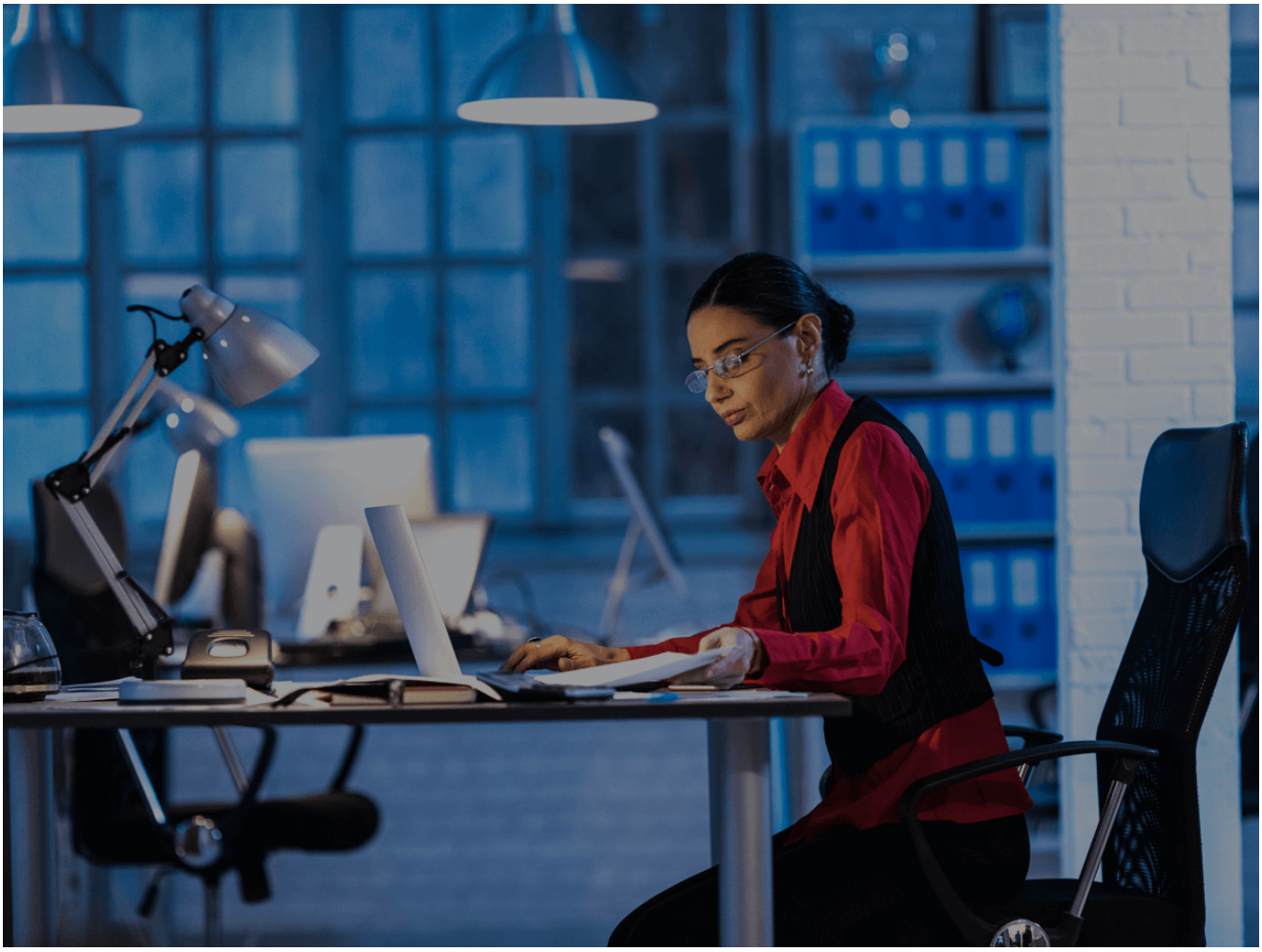
IZ1H9 Campaign Enhances Its Arsenal with Scores of Exploits

fortinet.com/blog/threat-research/Iz1h9-campaign-enhances-arsenal-with-scores-of-exploits

October 9, 2023



Affected Platforms: Linux
Impacted Users: Any organization
Impact: Remote attackers gain control of the vulnerable systems
Severity Level: Critical

In September 2023, our FortiGuard Labs team observed that the IZ1H9 Mirai-based DDoS campaign has aggressively updated its arsenal of exploits. Thirteen payloads were included in this variant, including D-Link devices, Netis wireless router, Sunhillo SureLine, Geutebruck IP camera, Yealink Device Management, Zyxel devices, TP-Link Archer, Korenix Jetwave, and TOTOLINK routers.

Based on the trigger counts recorded by our IPS signatures, it is evident that peak exploitation occurred on September 6, with trigger counts ranging from the thousands to even tens of thousands. This highlights the campaign's capacity to infect vulnerable devices and dramatically expand its botnet through the swift utilization of recently released exploit code, which encompasses numerous CVEs.

In this article, we will elaborate on how this threat leverages new vulnerabilities to control affected devices, along with the details of IZ1H9.

Figure 1: Telemetry

Exploit Payloads

Four payloads, CVE-2015-1187, CVE-2016-20017, CVE-2020-25506, and CVE-2021-45382, target D-Link vulnerabilities. These critical-severity vulnerabilities can allow remote attackers to deliver command injection via a crafted request.

Figure 2: D-Link exploit payload
Another exploit, CVE-2019-19356, targets Netis WF2419. It focuses on exploiting a Remote Code Execution (RCE) vulnerability through the tracert diagnostic tool because of a lack of user input sanitizing. The payload injects in parameter “tools_ip_url” and contains the “User-Agent: Dark” header used in the Dark.IoT Botnet.

Figure 3: Netis WF2419 exploit payload
The campaign also seeks to exploit vulnerabilities discovered in 2021, including CVE-2021-36380, which affect Sunhillo SureLine versions before 8.7.0.1.1, CVE-2021-33544/33548/33549/33550/33551/33552/33553/33554, which allow arbitrary command execution within the parameters of various pages on Geutebruck products, and CVE-2021-27561/27562, which affect Yealink Device Management (DM) 3.6.0.20.

Figure 4: Sunhillo/Geutebruck/Yealink exploit payload
The next exploit targets the Zyxel device’s /bin/zhttpd/ component vulnerability. If insufficient input validation is found, the attacker can exploit the vulnerability to launch a remote code execution attack on Zyxel EMG3525/VMG1312 before V5.50.

Figure 5: Zyxel exploit payload
The threat actor has also incorporated vulnerabilities discovered in 2023 into their exploit payload list. CVE-2023-1389 specifically targets TP-Link Archer AX21 (AX1800), while CVE-2023-23295 impacts Korenix JetWave wireless AP.

Figure 6: TP-Link/Korenix exploit payload
CVE-2022-40475/25080/25079/25081/25082/25078/25084/25077/25076/38511/25075/25083 collectively represent a set of related vulnerabilities that focus on TOTOLINK routers.

Figure 7: TOTOLINK exploit payload
The last one is an unclear exploit payload. It targets “/cgi-bin/login.cgi” and injects a payload in the “key” parameter. A similar vulnerability affects the Prolink PRC2402M router, but it is missing a few parameters to achieve remote code execution. It is unclear if the IZ1H9 campaign misused this payload or if they intended to target other devices.

Figure 8: Exploit payload targets login.cgi

Shell Script Downloader

The injected payload in the above vulnerabilities intends to get a shell script downloader “l.sh” from hxxp://194[.]180[.]48[.]100. When the script is executed, it begins by deleting logs to conceal its actions. It then downloads and executes various bot clients to cater to diverse Linux architectures. In the final step, the shell script downloader obstructs network connections on multiple ports. This is achieved by altering the device's iptables rules, as illustrated in Figure 9.

Figure 9: Shell script downloader "l.sh"

Malware Analysis - IZ1H9

IZ1H9, a Mirai variant, infects Linux-based networked devices, especially IoT devices, turning them into remote-controlled bots for large-scale network attacks. The XOR key to decode configuration is 0xBAADF00D, shown in Figure 10.

Figure 10: Decoding configuration
The additional payload downloader URLs can be extracted from the decoded configuration in Figure 11, namely hxxp://2[.]56[.]59[.]215/i.sh and hxxp://212[.]192[.]241[.]72/lolol.sh. Both were employed in May 2023.

Figure 11: Partial decoded configuration
IZ1H9 also includes a data section with pre-set login credentials for brute-force attacks. The XOR decoding key is 0x54, shown in Figure 12, and the decoded data is in Figure 13.

Figure 12: XOR decoding for login credentials

Figure 13: Decoded login credentials
As for the C2 communication, victims first send a check-in message with the parameter “l.expl” to the C2 server “194[.]180[.]48[.]101:5034,” and it responds with a keep-alive message “\x00\x00.” Once the compromised devices receive a command from the C2 server, shown in Figure 14, they parse the packet to determine the DDoS attack method, target host, and packet count, if specified, before launching the attack. The message structure is as follows:

- \x00\x28: Message packet length
- \x0c: TCP SYN Attack
- \x02: The following contains two options
- \x08\x12: Target + length
- \x68\x74\x74\x70\x73\x3a\x2f\x2f … \x69\x73: https://…is
- \x18\x04: Packet numbers + length
- \x35\x30\x30\x30: 5000 packets

Figure 14: C2 communication

Figure 15: TCP SYN flood attack

Figure 16: DDoS attacking methods

Conclusion

IoT devices have long been an attractive target for threat actors, with remote code execution attacks posing the most common and concerning threats to both IoT devices and Linux servers. The exposure of vulnerable devices can result in severe security risks. Despite the availability of patches for these vulnerabilities, the number of exploit triggers remains alarmingly high, often numbering in the thousands.

What amplifies the impact of the IZ1H9 Campaign are the rapid updates to the vulnerabilities it exploits. Once an attacker gains control of a vulnerable device, they can incorporate these newly compromised devices into their botnet, enabling them to launch further attacks like DDoS attacks and brute-force.

To counter this threat, it is strongly recommended that organizations promptly apply patches when available and always change default login credentials for devices.

Fortinet Protections

The malware described in this report are detected and blocked by FortiGuard Antivirus as:

BASH/Mirai.AEH!tr.dldr
ELF/Mirai.AT!tr
ELF/Mirai.GG!tr
Linux/Mirai.L!tr
Linux/Mirai.REAL!tr
Linux/Mirai.IZ1H9!tr

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard AntiVirus service. The FortiGuard AntiVirus engine is a part of each of those solutions. As a result, customers who have these products with up-to-date protections are protected.

Fortinet has also released IPS signatures to proactively protect our customers from the threats contained in the exploit list.

The URLs are rated as “Malicious Websites” by the FortiGuard Web Filtering service.

We also suggest our readers go through the free NSE training: NSE 1 – Information Security Awareness, a module on Internet threats designed to help end users learn how to identify and protect themselves from phishing attacks.

FortiGuard IP Reputation and Anti-Botnet Security Service proactively block these attacks by aggregating malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

If you believe this or any other cybersecurity threat has impacted your organization, please contact our Global FortiGuard Incident Response Team.

IOCs

URLs:

194[.]180[.]48[.]100
2[.]56[.]59[.]215
212[.]192[.]241[.]72

Files:

c8cf29e56760c50fa815a0c1c14c17641f01b9c6a4aed3e0517e2ca722238f63
1e15d7cd0b4682a86620b3046548bdf3f39c969324a85755216c2a526d784c0d
7b9dce89619c16ac7d2e128749ad92444fe33654792a8b9ed2a3bce1fee82e6a
b5daf57827ced323a39261a7e19f5551071b5095f0973f1397d5e4c2fcc39930
b523ea86ebfd666153078593476ca9bd069d6f37fa7846af9e53b1e01c977a17
8d07f15dd7d055b16d50cb271995b768fdd3ca6be121f6a35b61b917dfa33938
34628bcfc40218095c65678b52ce13cea4904ce966d0fd47e691c3cb039871ec
afc176f7b692a5ff93c7c66eee4941acf1b886ee9f4c070faf043b16f7e65c11
df9ee47c783fbe8c3301ed519033fc92b05d7fd272d35c64b424a7e46c6da43b
737ba9e84b5166134d491193be3305afa273733c35c028114d8b1f092940b9a3
0aa9836174f231074d4d55c819f6f1570a24bc3ed4d9dd5667a04664acb57147