Security Advisory 2022-035

Critical Remote Code Execution in Zyxel Products

May 17, 2022 — v1.0

TLP:WHITE

History:

- *17/05/2022 — v1.0 – Initial publication*

Summary

In April 2022, a security researcher from Rapid7 discovered and reported a vulnerability that affects Zyxel firewall and VPN devices for business (advisory publicly released on 12th May 2022). Tracked as CVE-2022-30525 with a CVSS score of 9.8, a successful exploitation of this vulnerability allows an **unauthenticated and remote** attacker to achieve **code execution** as the `nobody` user [1].

A public exploit is available and a module had been added to the Metasploit penetration testing framework. This vulnerability is currently exploited in the wild by attackers to get access to information systems [2].

It is **strongly** recommended to apply the vendor patch as soon as possible.

Technical Details

The affected products are vulnerable to unauthenticated and remote command injection via the administrative HTTP interface. This vulnerability is exploited through the `/ztp/cgi-bin/handler` URI and is the result of passing unsanitized attacker input into the `os.system` method in `lib_wan_settings.py`. The vulnerable functionality is invoked in association with the `setWanPortSt` command. An attacker can inject arbitrary commands into the `mtu` or the `data` parameter [1].

Affected Products

The list of affected products is following [2]:

Affected Models	Impacted version	Fixed Version
USG FLEX 100, 100W, 200, 500, 700	ZLD5.00 through ZLD5.21 Patch 1	ZLD V5.30
USG FLEX 50(W), USG20(W)-VPN	ZLD5.10 through ZLD5.21 Patch 1	ZLD V5.30
ATP series	ZLD5.10 through ZLD5.21 Patch 1	ZLD V5.30
VPN series	ZLD V4.60 through ZLD V5.21 Patch 1	ZLD V5.30

Recommendations

CERT-EU strongly recommends to apply the vendor patch as soon as possible. It can be done by enabling automatic firmware update.

References

[1] https://www.rapid7.com/blog/post/2022/05/12/cve-2022-30525-fixed-zyxel-firewall-unauthenticated-remote-command-injection/

[2] https://www.bleepingcomputer.com/news/security/hackers-are-exploiting-critical-bug-in-zyxel-firewalls-and-vpns/