Hive Pro

THREAT ADVISORY

Authentication Bypass Vulnerability in Zyxel Firmware

TA2022087

Threat Level AMBER

Publish Date – April 1, 2022

A severe vulnerability (CVE-2022-0342) has been discovered in the firmware of some of Zyxel's business-grade firewall and VPN products, potentially allowing attackers administrator-level access to affected devices. This vulnerability affects the USG/ZyWALL, USG FLEX, ATP, VPN, and NSG (Nebula Security Gateway) range of Zyxel products.

This is an authentication bypass vulnerability (CVE-2022-0342) discovered in the CGI program of some firewall versions due to a lack of a proper access control mechanism. An attacker could use this flaw to circumvent authentication and get administrative access to the device.

For optimal protection, we suggest organizations to update the firmware of their products according to the information given below.

Potential MITRE ATT&CK TTPs are:
TA0001: Initial Access
TA0002: Execution
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0006: Credential Access
TA0007: Discovery
TA0042: Resource Development
T1040: Network Sniffing
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
T1548: Abuse Elevation Control Mechanism
T1190: Exploit Public-Facing Application

Vulnerability Details

CVE ID	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0342	cpe:2.3:a:zyxel:*:*:*:*:*:*:*:*:*	Improper Authentication	CWE-287

Affected Products

Affected Series	Affected Firmware Version	Patch Availability
USG/ZyWALL	ZLD V4.20 through ZLD V4.70	ZLD V4.71
USG FLEX	ZLD V4.50 through ZLD V5.20	ZLD V5.21 Patch 1
ATP	ZLD V4.32 through ZLD V5.20	ZLD V5.21 Patch 1
VPN	ZLD V4.30 through ZLD V5.20	ZLD V5.21
NSG	V1.20 through V1.33 Patch 4	Hotfix V1.33p4_WK11* available now Standard patch V1.33 Patch 5 in May 2022

Patch Link

https://support.zyxel.eu/hc/en-us/articles/4672704562578-USG-FLEX-ATP-Series-Firmware-Update-5-21-Patch-1-Installation-Notes

References

https://www.zyxel.com/support/Zyxel-security-advisory-for-authentication-bypass-vulnerability-of-firewalls.shtml