مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Application Signature Issue in Zyxel USG FLEX ATP Series Firewalls
Tracking #:432316790
Date:27-01-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical issue has been identified affecting Zyxel USG FLEX and ATP Series firewalls with active security licenses.

TECHNICAL DETAILS:

A critical issue has been identified affecting Zyxel USG FLEX and ATP Series firewalls with active security licenses. The problem, which emerged on January 24th, 2025, was caused by a faulty Application Signature Update (version 1.0.0.20250123.0). This issue led to severe operational disruptions, including reboot loops, ZySH daemon failures, and login access problems. While not related to a CVE or security vulnerability, the impact on affected devices was significant and required immediate attention.

Key Details:
- Affected Devices: USG FLEX and ATP Series with active security licenses, running in On-premise/Standalone Mode
- Unaffected Devices: Nebula platform, USG FLEX H (uOS) series, and devices without active security licenses
- Root Cause: Failure in Application Signature Update (version 1.0.0.20250123.0)
- Symptoms: Reboot loops, high CPU usage, ZySH daemon failures, login access issues, system LED flashing

Current Status: As of January 27, 2025, Zyxel has,
- Removed the problematic App Patrol signature release V1.0.0.20250123.03.
- Disabled application signing on company servers to prevent further impacts
- Released urgent date firmware for affected devices to aid in recovery.
- Provided detailed recovery steps for on-site resolution

RECOMMENDATIONS:

- Immediate Assessment: Check the App-Patrol signature version is problematic version.
- On-Site Recovery: Perform the recovery process on-site using a console cable. Remote recovery attempts are not recommended

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- http://support.zyxel.eu/hc/en-us/articles/24159250192658-USG-FLEX-ATP-Series-Recovery-Steps-for-Application-Signature-Issue-on-January-24th