مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability in Four-Faith Routers

Tracking #:432316697

Date:03-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability has been discovered in Four-Faith routers that allows attackers to execute arbitrary OS commands remotely, potentially leading to full device compromise and is actively being exploited in the wild.

TECHNICAL DETAILS:

A vulnerability has been discovered in Four-Faith routers, specifically models F3x24 and F3x36. This flaw allows attackers to execute arbitrary OS commands remotely, potentially leading to full device compromise. The vulnerability is actively being exploited in the wild.

Key Details

- CVE ID: **CVE-2024-12856**
- Affected Devices: Four-Faith router models F3x24 and F3x36
- Vulnerability: OS command injection via the /apply.cgi endpoint
- CVSS Score: 7.2 (High)
- Exploitation: Active in-the-wild exploitation observed
- Exploitation Method: Attackers exploit this vulnerability by sending a crafted HTTP POST request to the /apply.cgi endpoint. The malicious payload is injected into the adj_time_year parameter, allowing the execution of arbitrary OS commands. If successful, the attacker can establish a reverse shell, gaining remote access to the device.

RECOMMENDATIONS:

1. Update Router Firmware:
    - Ensure all Four-Faith routers are running the latest firmware versions provided by the manufacturer. This may include patches that address CVE-2024-12856. Contact Four-Faith support to confirm the availability of firmware updates.
2. Change Default Credentials:
    - Replace any default usernames and passwords with strong, unique credentials for all affected devices.
3. Restrict Internet Exposure:
    - Limit internet-facing access to Four-Faith routers by using firewalls, VPNs, or other network security measures. Ensure that only trusted internal networks or authorized IP addresses can access the devices.
4. Monitor for Exploit Attempts:
    - Utilize Intrusion Detection Systems (IDS) or custom detection rules to identify any signs of exploitation attempts.

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:

- https://vulncheck.com/blog/four-faith-cve-2024-12856