مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Four-Faith F3x36 Routers

Tracking #:432316840
Date:07-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in Four-Faith F3x36 routers that could potentially be exploited to gain complete control of the affected devices.

TECHNICAL DETAILS:

Critical authentication bypass vulnerabilities (CVE-2024-9643 and CVE-2024-9644) exists in Four-Faith F3x36 routers running firmware **v2.0.0**. These flaws allow remote attackers to bypass authentication mechanisms and gain full administrative control of affected devices. Both vulnerabilities carry a **CVSS v3.1 score of 9.8 (Critical)**, underscoring their severe risk to network security.

Vulnerability Details:

CVE-2024-9643: Hard-Coded Credentials in Administrative Web Server

- This vulnerability is due to the presence of hard-coded credentials within the router's administrative web server. An attacker with knowledge of these credentials can bypass authentication and gain full administrative control by sending specially crafted HTTP requests. This issue is similar to previously reported hard-coded credential vulnerabilities (e.g., CVE-2023-32645).

CVE-2024-9644: Authentication Bypass via "bapply.cgi" Endpoint

- An authentication bypass vulnerability exists in the "bapply.cgi" endpoint of the administrative web server. This endpoint lacks proper authentication enforcement for certain administrative functions, allowing unauthenticated remote attackers to modify router settings. This vulnerability can also be chained with other vulnerabilities for even greater impact.

Affected Products:

- **Four-Faith F3x36 Series Routers**
  - Firmware Version: **v2.0.0**

RECOMMENDATIONS:

1. **Update Firmware:** Apply the latest firmware updates from Four-Faith.
2. **Restrict Network Access:** Limit remote access to administrative interfaces to trusted IPs.
3. **Disable Unused Services:** If remote administration is unnecessary, disable it to reduce exposure.
4. **Monitor Network Traffic:** Watch for unusual login attempts or unauthorized configuration changes.
5. **Change Default Credentials:** Ensure all default credentials are modified, even if a patch is applied.

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://nvd.nist.gov/vuln/detail/CVE-2024-9643
- https://nvd.nist.gov/vuln/detail/CVE-2024-9644