مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Stored XSS Vulnerability in IPFire Web Interface

Tracking #:432317649

Date:29-08-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability has been identified in the IPFire web-based firewall management interface (firewall.cgi).

TECHNICAL DETAILS:

A critical vulnerability has been discovered in IPFire 2.29's web-based firewall interface (firewall.cgi). The flaw allows authenticated administrators to inject persistent JavaScript payloads into firewall rules, resulting in a stored cross-site scripting (XSS) vulnerability. Exploitation could lead to session hijacking, unauthorized administrative actions, and lateral movement within internal networks.

Administrators are strongly urged to treat this as a high-priority security risk and apply mitigations immediately.

Vulnerability Details

- **CVE ID:** CVE-2025-50975
- **Affected Version:** IPFire 2.29
- **Vulnerability Type:** Stored Cross-Site Scripting (XSS)
- **Attack Vector:** Web Interface
- **Complexity:** Low
- **Impact:** Confidentiality & Integrity

An attacker with **GUI administrative access** can embed malicious JavaScript code into these fields. Once stored, the payload executes whenever another administrator views the firewall rules, enabling:

- **Session hijacking** via cookie theft
- **Unauthorized administrative actions** (e.g., modifying firewall rules)
- **Further attacks** on internal network systems

A demonstration of the stored XSS attack is available as a GIF proof-of-concept hosted on GitHub. The attack occurs immediately during rule creation and executes upon page reload in other sessions.

Attack Scenario

1. Attacker logs in to the IPFire web interface with administrator privileges.
2. Malicious JavaScript is injected into one or more firewall rule parameters.
3. The script is stored in the system and executes when other administrators view the firewall rules.
4. Consequences include theft of session cookies, unauthorized changes, or pivoting to internal resources.

RECOMMENDATIONS:

1. **Update IPFire:**
   - Apply the latest security patches or upgrade to a version beyond **2.29**, where input validation has been strengthened.
2. **Restrict Admin Access:**
   - Limit GUI-privileged users.
   - Enforce multi-factor authentication (MFA) for all administrative accounts.

3. **Implement Content Security Policy (CSP):**
    - Deploy a strict CSP header to restrict inline script execution and mitigate XSS impact.
4. **Audit Firewall Rules:**
    - Regularly review existing rules for anomalous characters or embedded scripts.
    - Remove any suspicious or unexpected payloads.
5. **Monitor and Respond:**
    - Observe administrator sessions for unusual activity.
    - Consider session invalidation or password resets if compromise is suspected.

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-2025-50975