CIRT.GY Guyana National Computer Incident Response Team

AL2025_36 FortiWeb CVE-2025-52970 Exploit Released: Full Authentication Bypass Risk (August 18, 2025)

Description

A newly disclosed vulnerability in Fortinet's FortiWeb Web Application Firewall (WAF), tracked as CVE-2025-52970, allows remote attackers to fully bypass authentication and impersonate any active user, including administrators. This flaw was dubbed FortMajeure. The vulnerability stems from an out-of-bounds read in FortiWeb's cookie parsing mechanism. By manipulating the `Era` parameter in session cookies, attackers can trigger a condition where FortiWeb falls back to using an all-zero secret key for session encryption and HMAC signing. This effectively renders session cookies forgeable. Although Fortinet issued a patch on August 12, 2025, researchers have already released a partial proof-of-concept (PoC) exploit, raising concerns about imminent weaponization.

Attack Details

The vulnerability in FortiWeb, tracked as CVE-2025-52970, stems from a flaw in cookie handling where malicious modification of the Era cookie parameter forces the system to use an all-zero cryptographic key, allowing attackers to forge authentication cookies and impersonate active users. To exploit this issue, a target user must have an active session, and the attacker must brute-force a small numeric field in the signed cookie validated by the function refresh_total_logins() in libncfg.so. Since the field typically falls within a range of 30 values or fewer, the brute-force stage is trivial, requiring only about 30 requests. Successful exploitation results in a full authentication bypass, enabling attackers to impersonate administrators, gain unauthorized access to REST endpoints, and potentially connect to the CLI via /ws/cli/open. The flaw impacts FortiWeb versions 7.0 to 7.6, with patches available in 7.0.11, 7.2.11, 7.4.8, and 7.6.4 or later, while FortiWeb 8.0 releases remain unaffected.

Remediation

1. **Upgrade immediately** to fixed FortiWeb versions:
    a. 7.6.4 or later
    b. 7.4.8 or later
    c. 7.2.11 or later
    d. 7.0.11 or later
2. **Verify user sessions:**
    a. Terminate all existing sessions after patching.
    b. Force users to re-authenticate.
3. **Harden monitoring:**
    a. Enable logging for all authentication events.
    b. Deploy anomaly detection on cookie values and session activity.
4. **Restrict management access:**
    a. Limit administrative access to trusted IPs only.
    b. Consider enabling multi-factor authentication (MFA) where supported.
5. **Prepare for PoC release:**

a. Although the full exploit has not yet been published, attackers are likely working on weaponization.
b. Apply patches urgently to avoid exposure when the exploit becomes public.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B. (2025, August 15). Researcher to release exploit for full auth bypass on FortiWeb. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/researcher-to-release-exploit-for-full-auth-bypass-on-fortiweb/all-confirms-patched.html?m=1
- PSIRT | FortiGuard Labs. (n.d.). Retrieved from FortiGuard Labs. https://fortiguard.fortinet.com/psirt/FG-IR-25-448