

## FortiOS CVE's

**WE Innovate X Zero\$exploit**

*Supervised by : Mohamed Badawy*

*Prepared by: Omar Hassan – Ali Abdelrahman – Ahmed Taha – Omar Tarek –  
Noha Sayed – Rami Khaled*



This report provides an overview of recent FortiOS vulnerabilities (CVEs), their impacts, proof-of-concept (PoC) exploit availability, and recommended mitigations.

### 1. CVE-2024-55591

Type: Authentication Bypass via Alternate Path or Channel (CWE-288)

Affected Versions: FortiOS 7.0.0 through 7.0.16, FortiProxy 7.0.0–7.0.19 and 7.2.0–7.2.12

Impact: Remote attacker can gain super-admin privileges by sending crafted WebSocket requests.

Exploit Activity: Actively exploited in the wild since November 2024.

CVSS Score: 9.6 (Critical)

#### PoCs:

- virus-or-not/CVE-2024-55591: <https://github.com/virus-or-not/CVE-2024-55591>
- watchtowrlabs PoC: <https://github.com/watchtowrlabs/fortios-auth-bypass-poc-CVE-2024-55591>
- Technical Analysis: [https://labs.watchtowr.com/get-fortirekt-i-am-the-super\\_admin-now-fortios-authentication-bypass-cve-2024-55591/](https://labs.watchtowr.com/get-fortirekt-i-am-the-super_admin-now-fortios-authentication-bypass-cve-2024-55591/)

### 2. CVE-2025-24472

Type: Authentication Bypass via CSF Proxy Requests (CWE-288)

Affected Versions: FortiOS 7.0.0–7.0.16, FortiProxy 7.0.0–7.0.19 and 7.2.0–7.2.12

Impact: Requires knowledge of device serial numbers; allows super-admin access in Security Fabric setups.

PoC: No public PoC available as of now.

### 3. Other Recent FortiOS CVEs

- CVE-2025-47295: Buffer over-read in FGFM daemon (DoS).
- CVE-2025-47294: Integer overflow in csfd daemon (crash possible).
- CVE-2024-52965: Auth bypass with invalid cert + API key.
- CVE-2024-52963: Out-of-bounds write (DoS).
- CVE-2024-50568: Security Fabric spoofing (unauthenticated TCP attack).
- CVE-2024-50565: FGFM channel restriction bypass (MITM risk).
- CVE-2024-50562: Insufficient SSL-VPN session expiration (reuse of expired cookies).

## 4. Mitigation & Recommendations

1. Patch systems immediately:
  - FortiOS 7.0.17+
  - FortiProxy 7.0.20+ or 7.2.13+
2. Monitor logs for suspicious admin logins and anomalies.
3. Restrict HTTP/HTTPS admin access to trusted IPs.
4. Assume compromise if systems were unpatched during active exploitation.

## Summary

- **Most critical:** CVE-2024-55591 — *Authentication Bypass*, active exploitation, multiple public PoCs.
- **Secondary critical:** CVE-2025-24472 — similar pattern but requires specific serial-number knowledge.
- **Other significant risks:** Several CVEs related to DoS, spoofing, session reuse, but no PoCs publicly noted yet.
- **Immediate steps:** Patch, monitor logs, enable workarounds, and assume exposure risk.