CYBER ADVISORY

Friday, November 14, 2025 **CAL-CSIC-202511-A-005**

FortiWeb Flaw Exploited to Create Admin Accounts

Authentication Bypass | Admin Account Creation | Proof-of-Concept | Zero-Day

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a potential zero-day critical vulnerability in the Fortinet FortiWeb product.[1] This vulnerability, whose CVE is still under review, arises from an authentication bypass vulnerability in FortiWeb versions prior to 8.0.2. Successful exploitation allows an adversary to create new administrator accounts on the appliance by sending crafted HTTP POST requests that exploit the management API endpoint, /api/v2.0/cmdb/system/admin%3F/../../../../../cgi-bin/fwbcgi. Once an admin account is created, the attacker gains full control of the device enabling them to undermine perimeter Web Application Firewall (WAF) protections and establish persistence.

Exploitation is confirmed in the wild and a Proof-of-Concept was published.[2][3] WatchTowr, a cybersecurity research group, has also published a detection artifact generator for FortiWeb authentication bypass on GitHub.[4] The vendor's fix is included in version 8.0.2 and instructions to upgrade can be found here.

The Cal-CSIC recommends immediately applying the latest FortiWeb patch due to the severity of the vulnerability and active exploitation documented in the wild.

Indicators-of-Compromise associated with this zero-day (IPs):

107.152.41.19	144.31.1.63	89.169.55.168	185.192.70.33	185.192.70.53
185.192.70.43	185.192.70.25	185.192.70.36	185.192.70.49	185.192.70.39
185.192.70.57	185.192.70.50	185.192.70.46	185.192.70.31	64.95.13.8

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Usernames and Passwords extracted from malicious payloads associated with this zero-day:

Username	Password
Testpoint	AFodIUU3Sszp5
trader1	3eMIXX43
trader	3eMIXX43
test1234point	AFT3$tH4ck
Testpoint	AFT3$tH4ck
Testpoint	AFT3$tH4ckmet0d4yaga!n

References

[1] Security Online; "ZERO-DAY ATTACK WARNING: Fortinet FortiWeb Exploit Grants Unauthenticated Admin Access!"; https://securityonline.info/zero-day-attack-warning-fortinet-fortiweb-exploit-grants-unauthenticated-admin-access/; accessed November 14, 2025
[2] watchTowr; "another exploited in-the-wild FortiWeb vuln? It must be Thursday!"; https://x.com/watchtowrcyber/status/1989017336632996337; accessed November 14, 2025
[3] pwndefend; "Suspected Fortinet zero day exploited in the wild"; https://www.pwndefend.com/2025/11/13/suspected-fortinet-zero-day-exploited-in-the-wild/; accessed November 14, 2025
[4] GitHub; "watchTowr-vs-Fortiweb-AuthBypass"; https://github.com/watchtowrlabs/watchTowr-vs-Fortiweb-AuthBypass; accessed November 14, 2025

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.