THREAT BULLETINS

Exploit Code Released for Fortinet FortiWeb Flaw CVE-2025-52970

TLP:WHITE

Aug 18, 2025

On August 12, 2025, FortiGuard Labs published an advisory for a flaw in FortiWeb tracked as CVE-2025-52970. Practical exploit code is now available for this flaw, increasing the possibility of attacks.

CVE-2025-52970 is an improper handling of parameters vulnerability in the FortiWeb web application firewall (WAF). This flaw allows an unauthenticated remote attacker to bypass authentication and gain administrative privileges. The attacker must possess non-public information pertaining to the device and the targeted user to exploit the vulnerability successfully. This suggests the attack requires some level of reconnaissance or insider knowledge. The CVSS score of the flaw is 7.7.

Affected Products:

- FortiWeb 7.6.0 through 7.6.3
- FortiWeb 7.4.0 through 7.4.7
- FortiWeb 7.2.0 through 7.2.10
- FortiWeb 7.0.0 through 7.0.10

Recommendations:

Health-ISAC is advising members with vulnerable FortiWeb devices to apply available patches immediately. If immediate patching is not feasible, an organization can reduce the attack surface by restricting access to the FortiWeb administrative interface. Additionally, it is advised to consult the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patient Resources.

Reference(s)	hhs, nist, pwner, fortinet, hkcert

Sources
https://www.hkcert.org/security-bulletin/fortinet-fortiweb-security-restriction-bypass-vulnerability_20250818

https://nvd.nist.gov/vuln/detail/CVE-2025-52970

https://fortiguard.fortinet.com/psirt/FG-IR-25-448

https://pwner.gg/blog/2025-08-13-fortiweb-cve-2025-52970

Incident Date
Aug 17, 2025 (UTC)

Alert ID bb2bcd9e

View Alert

Share Feedback
was this helpful? |

Tags CVE-2025-52970, FortiWeb Web Application Firewall (WAF), Fortinet

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.