VULNERABILITY BULLETINS

Zero-Day Exploitation of Fortinet FortiWeb Path Traversal Flaw

TLP:WHITE

Nov 14, 2025

On October 6, 2025, security researchers at Defused reported a path traversal flaw in Fortinet's FortiWeb web application firewall (WAF) being exploited in-the-wild as a zero-day since October 2025.

This unauthenticated flaw allows remote attackers to bypass security measures and successfully create new, privileged administrative accounts on exposed devices. Users are strongly encouraged to upgrade to the latest version (8.0.2) of FortiWeb to prevent unauthorized system access and compromise.

Health-ISAC is sharing this to increase situational awareness and encourage organizations to assess their level of risk to this vulnerability.

Analysis

The vulnerability is identified as a path traversal flaw affecting the FortiWeb appliance's management interface. Cybersecurity researchers at Defused were among the first to observe the exploitation, reporting an unknown Fortinet exploit being used against

exposed devices as early as October 6, 2025. Subsequently, the researchers published limited proof-of-concept (PoC) code to help defenders identify and mitigate the threat, leading to an increase in global exploitation attempts.

Exploitation of this zero-day flaw is conducted via threat actors sending HTTP POST requests to a specific path on the FortiWeb management interface: /api/v2.0/cmdb/system/admin%3f/../../../../../cgi-bin/fwbcgi. By sending a malicious payload to this endpoint, an attacker can bypass normal authentication mechanisms and directly execute commands related to user management. This capability is highly critical as it grants the attacker the ability to establish persistent, unauthorized access. Security researchers at both watchTowr Labs and Rapid7 have successfully confirmed the exploit vector and its effectiveness.

The primary consequence of successful exploitation is the creation of new, local admin-level accounts on the compromised FortiWeb appliance, without needing valid credentials. Observed attacks have used various credentials, with usernames like Testpoint, trader1, and trader, indicating that threat actors are systematically scanning for and backdooring vulnerable installations globally. This remote administrative access allows complete control over the web application firewall, enabling attackers to potentially steal configuration data or pivot into the protected network.

Fortinet has not yet publicly released a full advisory detailing the flaw, but a patch is available in the form of a specific fixed software release. The vulnerability affects FortiWeb versions 8.0.1 and earlier. Due to the active exploitation and the public availability of a PoC, patching is essential, as no configuration workarounds are available beyond strictly controlling network access.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Upgrade all vulnerable FortiWeb appliances to version 8.0.2 or newer.
- Ensure that the FortiWeb management interface is not exposed to the public internet.
- Leverage watchTowr Labs' FortiWeb Authentication Bypass Artifact Generator tool designed to help defenders identify vulnerable devices by attempting to trigger the exploit and check for specific indicators.
- Check for IOCs (Indicators of Compromise)
- Review device logs for suspicious HTTP requests targeting the /cgi-bin/fwbcgi path.
- Audit local user accounts for unauthorized administrator accounts, specifically looking for unfamiliar or recently created usernames (e.g., "Testpoint", "trader1").
- Investigate activity originating from reported suspicious IP addresses.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	pwndefend, hhs, x, bleepingcomputer, rapid7, github, helpnetsecurity, x 1, amazonaws

Alert ID fce20ca1

View Alert

Share Feedback

was this helpful? |

Tags Fortiweb, Fortinet

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

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

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/**