Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Service Finder Plugin Flaw Opens Door to Full Site Compromise

Date of Publication	Admiralty Code	TA Number
October 9, 2025	A1	TA2025309

Summary

Discovered On: June 8th, 2025
Affected Products: WordPress Service Finder Bookings Plugin
Impact: A critical flaw in the Service Finder Bookings plugin, tracked as CVE-2025-5947, is being actively exploited by attackers to bypass authentication and gain administrator access to WordPress sites. The issue stems from improper cookie validation in the plugin's account-switching feature, allowing unauthenticated users to impersonate admins and take full control of vulnerable sites. Although a patch was released in mid-July, exploitation began shortly after public disclosure, prompting thousands of attack attempts. Site owners are urged to update to version 6.1 or later and check for any signs of unauthorized activity.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-5947	WordPress Service Finder Bookings Plugin Authentication Bypass Vulnerability	WordPress Service Finder Bookings Plugin	✗	✗	✓

Vulnerability Details

#1 A critical flaw in the Service Finder Bookings plugin lets attackers bypass authentication and seize administrator accounts on sites using the Service Finder WordPress theme. Tracked as CVE-2025-5947, the vulnerability undermines the plugin's account-switching logic and exposes a tool widely used by service providers to manage appointments, schedules, and payments.

#2 At its core, the vulnerability stems from improper validation of cookie values in the plugin's service_finder_switch_back() routine. Because the code omits essential authentication and authorization checks, an unauthenticated actor can manipulate the flow to impersonate any user, including administrators enabling full site takeover, data modification, or malicious installations.

#3 The issue was reported through a bug-bounty submission on June 8, 2025, and impacts roughly 6,000 installations. A security update was published on July 17, 2025, with public disclosure on July 31, 2025; exploitation attempts were observed beginning August 1, 2025, prompting thousands of blocked hits flagged by security vendors.

#4 Site owners must update the Service Finder Bookings plugin to version 6.1 or later immediately. Beyond patching, administrators should audit access logs for signs of unauthorized activity, inspect user accounts for suspicious changes, and verify that all themes and plugins are up to date to remove lingering risk and restore secure operation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-5947	WordPress Service Finder Bookings Plugin Version Prior to 6.1	cpe:2.3:a:service_finder_bookings_plugin:service_finder_bookings_plugin:*:*:*:*:*:*:*:*	CWE-639

Recommendations

Update Immediately: Install the latest version of the Service Finder Bookings plugin (v6.1 or later) to close the authentication bypass flaw.

- **Don’t Rely Only on Firewalls:** While security plugins like Wordfence can block many attacks, updating the plugin itself is the only way to fully fix the issue.
- **Review Site Activity:** Check your WordPress logs and user accounts for any unusual logins or changes that might indicate compromise.
- **Strengthen Access Control:** Use strong, unique admin passwords and enable two-factor authentication to reduce the risk of unauthorized access in the future.
- **Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0004** Privilege Escalation	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1190** Exploit Public-Facing Application	**T1068** Exploitation for Privilege Escalation	**T1078** Valid Accounts

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	5[.]189[.]221[.]98, 185[.]109[.]21[.]157, 192[.]121[.]16[.]196, 194[.]68[.]32[.]71, 178[.]125[.]204[.]198

Patch Details

Updated your Service Finder Bookings Plugin to the latest version 6.1.

Link:
https://themeforest.net/item/service-finder-service-and-business-listing-wordpress-theme/15208793?srsltid=AfmBOoq5ifHWqLc8b5o0Q7gjSz6HEpbHfquXWh-KhP0FWnFBTCFLaBzH

References

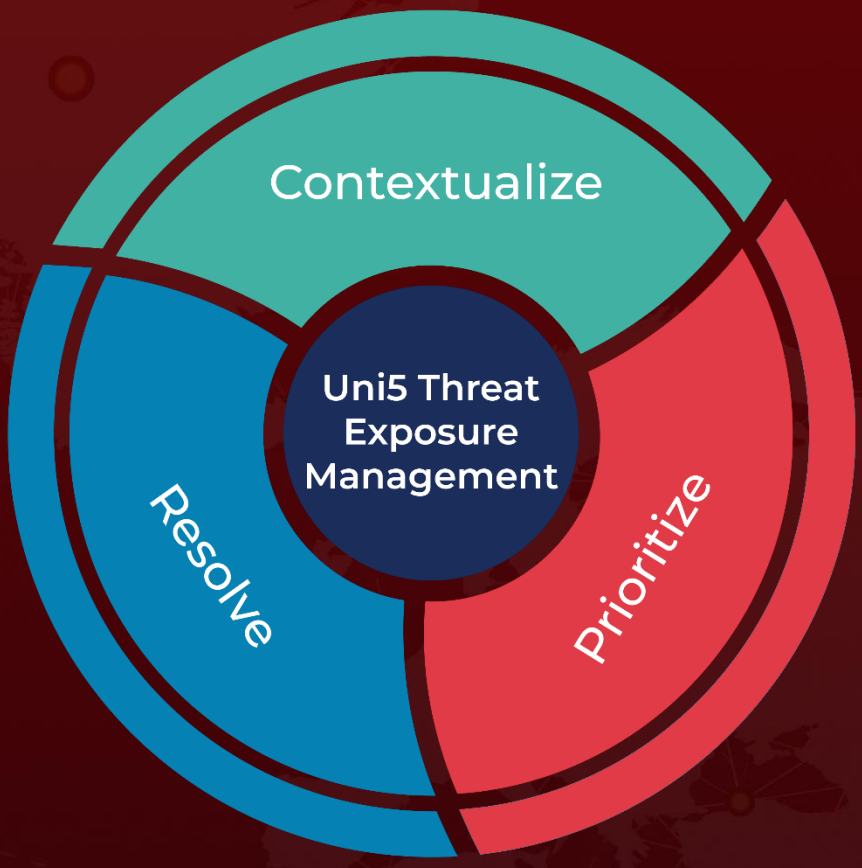
https://www.wordfence.com/blog/2025/10/attackers-actively-exploiting-critical-vulnerability-in-service-finder-bookings-plugin/

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/sf-booking/service-finder-bookings-60-authentication-bypass-via-user-switch-cookie

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 9, 2025 . 9:00 AM

More at www.hivepro.com