

**HiveForce Labs**

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **CVE-2025-3102: SureTriggers Plugin Flaw Lets Hackers Instantly Become Admins**

Date of Publication

April 11, 2025

Admiralty Code

A1

TA Number

TA2025112




# Summary

**First Seen:** March 13, 2025

**Affected Products:** SureTriggers

**Impact:** A high severity flaw in the OttoKit (formerly SureTriggers) WordPress plugin is being used in attacks just hours after it was disclosed. The flaw tracked as CVE-2025-3102 lets hackers break in and create admin accounts without logging in, but only if the plugin is installed and not fully set up with an API key. That tiny misstep opens the door to total site takeover, attackers can add users, install malicious plugins, deface content, or hijack your traffic.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-3102	SureTriggers Authorization Bypass Vulnerability	SureTriggers			

# Vulnerability Details

## #1

A newly disclosed critical vulnerability in SureTriggers is under active exploitation just hours after it went public. Tracked as CVE-2025-3102, the flaw affects the SureTriggers plugin for WordPress a popular no-code tool that lets users automate workflows across WordPress, plugins, and thousands of third-party services.

## #2

The vulnerability stems from a flaw in the plugin's authentication process. When the SureTriggers plugin is installed and activated but not yet configured with an API key it fails to properly validate the `secret_key` in its `authenticate_user()` function. This oversight allows attackers to bypass authentication simply by submitting an empty key, granting themselves full administrative access to the site.

## #3

The core issue is in the `run_action()` function within the plugin's `RestController` class, which handles automation events through the `automation/action` REST API endpoint. This endpoint relies on `authenticate_user()` for permission checks, but those checks are incomplete. Instead of validating whether the secret key is present and valid, it merely compares the submitted key against the (nonexistent) configured key. If no API key is set, the check passes by default, giving attackers access to perform admin-level actions like creating new users, installing malicious plugins or themes, injecting spam, or redirecting traffic to harmful sites.

## #4

This vulnerability only impacts fresh or misconfigured installations of the plugin but for those, the danger is significant. In fact, the first signs of exploitation emerged just four hours after the vulnerability was patched, proving how fast threat actors can strike. If you're using this plugin, patching immediately is critical to keeping your site secure.

## Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-3102	Suretriggers Prior to 1.0.79	cpe:2.3:a:suretriggers:suretriggers:*:*:*:*:*:*	CWE-697

## Recommendations



**Update the Plugin Without Delay:** If you have the SureTriggers or OttoKit plugin installed on your WordPress site, make sure to update it to the latest version as soon as possible. Hackers are already taking advantage of this security flaw, so staying on an older version could leave your site wide open to attacks.



**Look Out for Suspicious Admin Accounts:** Go through your WordPress user list and check if there are any administrator accounts you don't recognize. If you spot anything unusual, delete those accounts immediately. As an extra safety step, reset passwords for all admin users to keep your site secure.



**Secure Your Plugin Settings & Monitor for Threats:** Manually configure the plugin by setting a strong, unique API secret key this step is crucial, as the vulnerability stems from a missing or empty key. At the same time, keep an eye on your site's logs for suspicious activity, especially around the plugin's automation/action REST API endpoint or any unexpected user account creations.



**Deactivate the Plugin if Unused or Unconfigured:** If the plugin is installed but isn't being actively used or hasn't been fully set up with a secure API key it's safer to deactivate or remove it for now. Leaving it unconfigured leaves your site wide open to attack.



**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

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation
<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1068</u></b> Exploitation for Privilege Escalation
<b><u>T1556</u></b> Modify Authentication Process	<b><u>T1136</u></b> Create Account	<b><u>T1189</u></b> Drive-by Compromise	

## Indicator of Compromise (IOCs)

TYPE	VALUE
<b>IPv6</b>	2a01[:]e5c0[:]3167[::]2
<b>IPv4</b>	89[.]169[.]15[.]201
<b>URLs</b>	/?rest_route=/wp-json/sure-triggers/v1/automation/action, /wp-json/sure-triggers/v1/automation/action

## Patch Details

The vulnerability has been fixed in SureTriggers plugin version 1.0.79. If you're using an older version, update right away to keep your site protected from active exploitation.

Link: <https://wordpress.org/plugins/suretriggers/>

## References

<https://www.wordfence.com/blog/2025/04/100000-wordpress-sites-affected-by-administrative-user-creation-vulnerability-in-suretriggers-wordpress-plugin/>

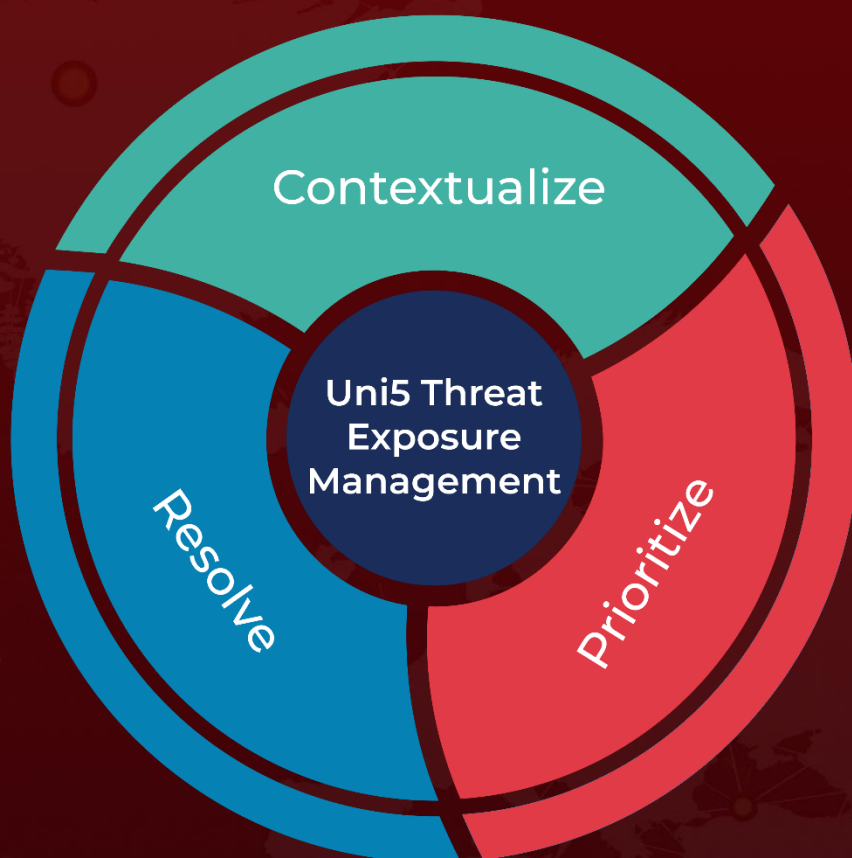
<https://patchstack.com/articles/critical-suretriggers-plugin-vulnerability-exploited-within-4-hours/>



# 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

**April 11, 2025 • 5:20 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)