

**THREAT ADVISORY**



**VULNERABILITY  
REPORT**

**New vulnerability allows attackers to  
takeover entire WordPress website**

Date of Publication

June 21, 2022

Admiralty code

A1


TA Number

TA2022127

# Summary

An unauthenticated attacker can call multiple methods in Ninja Forms class in order to inject object to eventually perform Remote Code Execution(RCE).

## CVEs

CVE	NAME	PATCH
Unassigned	Code Injection	

## Potential MITRE ATT&CK TTPs

<b>TA0002</b> Execution	<b>T1059</b> Command and Scripting Interpreter	<b>T1203</b> Exploitation for Client Execution	<b>TA0005</b> Defense Evasion
<b>T1055</b> Process Injection	<b>TA0011</b> Command and Control	<b>T1102</b> Web Service	<b>TA0042</b> Resource Development
<b>T1587</b> Develop Capabilities			

# Technical Details

An unauthenticated attacker can exploit this object injection vulnerability by calling several methods in various WordPress Ninja Forms classes, one of the methods used by the attacker could be the unserialized user supplied content. This allows the attacker to execute arbitrary codes and delete files, which leads to the takeover of vulnerable WordPress websites by performing RCE

## Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
Unassigned CVE ID	3.6-3.6.10, 3.5-3.5.8.3, 3.4-3.4.34.1, 3.3-3.3.21.3, 3.2-3.2.27, 3.1-3.1.9, 3.0-3.0.34.1	cpe:2.3:a:ninjaforms:ninja_forms:*:*:*:*:wordpress:*.*	CWE-94

## Patch Details

Update to versions 3.0.34.2, 3.1.10, 3.2.28, 3.3.21.4, 3.4.34.2, 3.5.8.4, 3.6.11

## References

<https://www.wordfence.com/blog/2022/06/psa-critical-vulnerability-patched-in-ninja-forms-wordpress-plugin/>

<https://thehackernews.com/2022/06/over-million-wordpress-sites-forcibly.html>

# What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.



At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

**June 21, 2022 • 4:15 AM**

© 2022 All Rights are Reserved by HivePro



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