Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

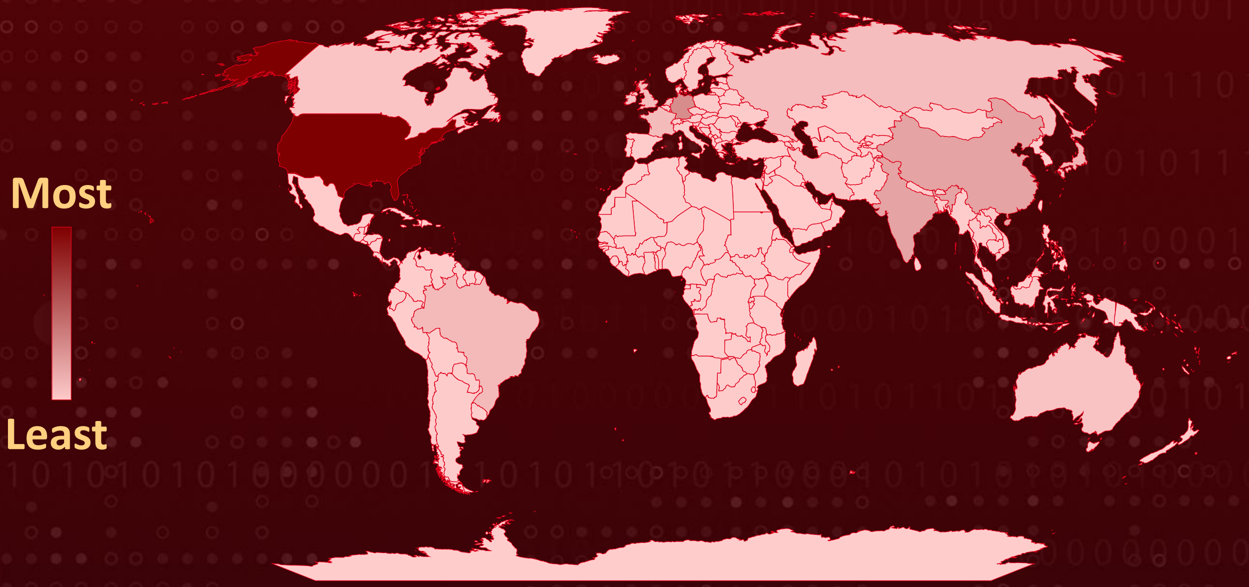
Next.js Under Siege as CVE-2025-29927 Opens the Floodgates for Attackers

Date of Publication	Admiralty Code	TA Number
March 26, 2025	A1	TA2025096

Summary

Discovered On: February 27, 2025
Affected Product: Next.js
Targeted Region: Worldwide
Impact: A newly discovered vulnerability, CVE-2025-29927, has shaken the foundations of Next.js middleware, leaving millions of applications exposed. This flaw grants attackers the power to bypass security controls using nothing more than a manipulated HTTP header. Given Next.js's widespread adoption, the potential damage is vast. From unauthorized access to malicious content injection, the consequences are severe. Organizations relying on Next.js are urged to act swiftly; in the face of such a simple yet devastating exploit, every second counts.

Targeted Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-29927	Next.js Middleware Bypass Vulnerability	Next.js React framework	✗	✗	✓

Vulnerability Details

#1

A critical vulnerability, ***CVE-2025-29927***, has been unearthed in ***Next.js middleware***, exposing countless applications to attack. With ***no prerequisites for exploitation***, the bug poses a severe risk. Given that Next.js is downloaded nearly ***10 million times weekly*** and supports applications across industries, including the emerging Web3 space, the potential fallout is significant.

#2

Middleware allows developers to inspect, modify, or block requests as they pass through, often acting as the first line of defense for authentication, authorization, and security enforcement. However, a subtle flaw within this system has shattered those defenses.

#3

The vulnerability stems from the misuse of the ***x-middleware-subrequest*** header a mechanism designed to prevent endless request loops during middleware execution. When a request reaches a Next.js application, the middleware uses a function called ***runMiddleware()*** to evaluate it. If the x-middleware-subrequest header is present and contains a specific value, the middleware execution is skipped entirely, and the request proceeds to its intended destination without further scrutiny.

#4

This mechanism can be easily bypassed, no complex hacking tools are needed just a single, well-crafted HTTP request. With the guardrails down, attackers have free rein. The implications are severe. A single manipulated request can bypass authentication and authorization checks, granting attackers access to restricted areas.

#5

If the security policies rely on middleware to apply Content Security Policy (CSP) headers, attackers can strip them away, opening the door for malicious scripts and potential Cross-Site Scripting (XSS) attacks. Worse yet, with middleware controls disabled, cache mechanisms are left exposed. Attackers could inject harmful content into the cache, causing a Denial of Service (DoS) or spreading malicious data to unsuspecting users.

#6

This vulnerability is particularly dangerous due to its ease of exploitation. Without specialized tools or expertise, even low-level attackers can bypass core security mechanisms using nothing more than a manipulated HTTP header. For organizations relying on Next.js, the urgency to patch this flaw cannot be overstated.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-29927	Next.js versions prior to 12.3.5 and after 11.1.4, prior to 14.2.25 and after 14.0, prior to 15.2.3 and after 15.0, prior to 13.5.9 and after 13.0.0	cpe:2.3:a:vercel:next.js:-:*:*:*:*:*:*:*	CWE-285

Recommendations

Apply Official Patches: The most effective way to mitigate the vulnerability is by updating your Next.js application to a patched version. Vercel has resolved the issue in the following releases:

- Next.js 15.x: Fixed in 15.2.3
- Next.js 14.x: Fixed in 14.2.25
- Next.js 13.x: Fixed in 13.5.9
- Next.js 12.x: Fixed in 12.3.5
- Next.js 11.x: Apply the recommended workaround provided below.

Implement a Temporary Workaround: If immediate updates aren't possible, mitigate the vulnerability by blocking or stripping the ***x-middleware-subrequest*** header. For applications behind load balancers like AWS ELB, Cloudflare, or Azure Front Door, configure rules to remove the header from incoming requests. On Nginx, use ***proxy_set_header x-middleware-subrequest "";*** and on Apache, apply ***RequestHeader unset x-middleware-subrequest*** to prevent exploitation. These workarounds effectively prevent malicious requests from exploiting the vulnerability until the application is updated to a patched version.

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

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0040 Impact	**T1059** Command and Scripting Interpreter	**T1505** Server Software Component	**T1553** Subvert Trust Controls
T1574 Hijack Execution Flow	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1498** Network Denial of Service

Patch Links

https://github.com/vercel/next.js/releases

https://github.com/vercel/next.js/security/advisories/GHSA-f82v-jwr5-mffw

References

https://zhero-web-sec.github.io/research-and-things/nextjs-and-the-corrupt-middleware

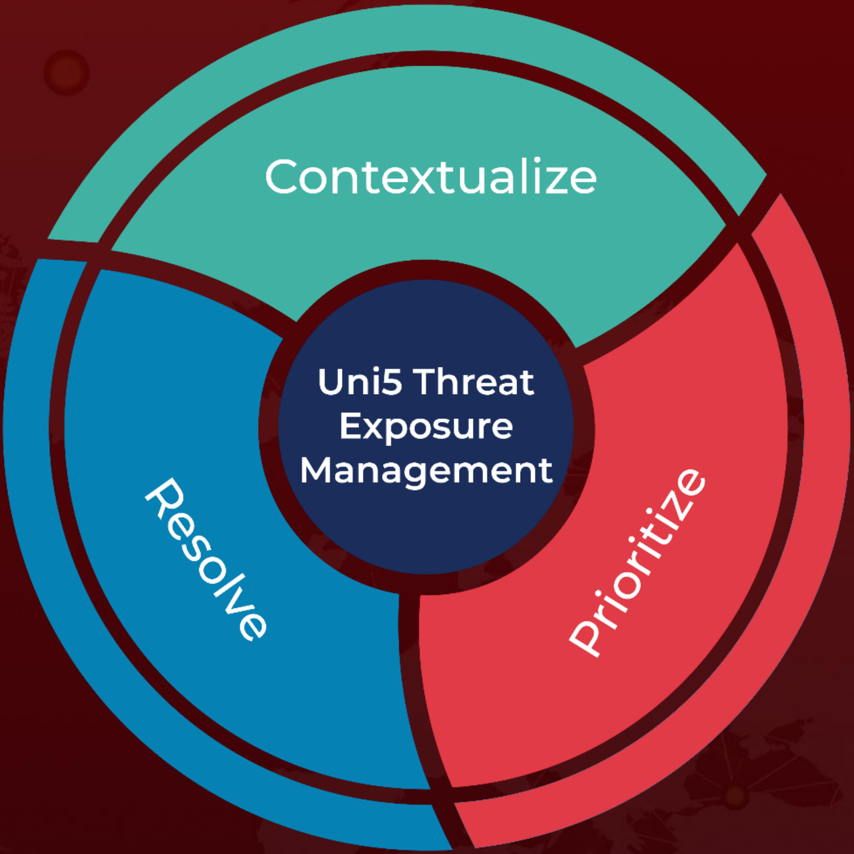
https://nextjs.org/blog/cve-2025-29927

https://nextjs.org/docs/app/building-your-application/routing/middleware

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

March 26, 2025 • 10:00 PM

More at www.hivepro.com