VULNERABILITY BULLETINS

Critical Authorization Bypass Vulnerability Announced For Next.js Middleware (CVE-2025-29927)

TLP:WHITE

Mar 26, 2025

On March 23, 2025, a critical vulnerability in Next.js middleware was disclosed and tracked as CVE-2025-29927. The vulnerability has a critical CVSS score of 9.1 and allows attackers to bypass authorization checks by adding a specially crafted request header to HTTP requests.

The vulnerability affects the following versions of Next.js:

- 11.1.4 through 13.5.6
- 14.x before 14.2.25
- 15.x before 15.2.3.

This flaw allows attackers to bypass middleware authorization checks under specific conditions, potentially exposing sensitive resources such as admin pages or other high-privilege areas.

Given the health sector's reliance on web applications for patient portals, administrative dashboards, and other critical services, this vulnerability poses a significant potential risk.

Health-ISAC has identified several member organizations with environments that leverage Next.js. Targeted Alerts have been delivered to those organizations where visibility into Next.js usage was evident. The Targeted Alerts are based on the presence of Next.js rather than the presence of an impacted version.

Health-ISAC does not have visibility into the version of Next.js detected and is providing alerts out of an abundance of caution to ensure appropriate actions are taken. Your team will need to determine which version is currently in use.

Analysis:

Next.js usage is prevalent in many health sector environments. CVE-2025-29927 represents a critical threat to organizations in the health sector, particularly those relying on Next.js for web applications.

Immediate action is required to patch vulnerable systems, implement temporary mitigations, and strengthen overall security posture.

Failure to address this vulnerability could result in unauthorized access to sensitive data, operational disruptions, and regulatory non-compliance.

Recommendations:

If patching to a safe version is infeasible, it is recommended that you prevent external user requests that contain the x-middleware-subrequest header from reaching your Next.js application. This vulnerability is fixed in versions 14.2.25 and 15.2.3.

ProjectDiscovery has provided a detailed analysis and a workaround for the authorization bypass vulnerability.

Health-ISAC provides this information to prevent your security apparatus's successful exploitation and disruption. For more information, see Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients.

References:

https://projectdiscovery.io/blog/nextjs-middleware-authorization-bypass
https://nvd.nist.gov/vuln/detail/CVE-2025-29927

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-29927

Reference(s)	Mitre, NIST-CSF,

Release Date
Mar 27, 2025 (UTC)

Alert ID 0f1c9208

View Alert

Share Feedback
was this helpful? |

Tags ProjectDiscovery, CVE-2025-29927, Next.js

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/**