

Forum:[Hack Forums](#)

Thread: [Apache NiFi Vulnerability Exposes MongoDB Usernames and Passwords to Attackers](#)

JoseMar - March 13, 2025, 9:48 am

Apache NiFi Vulnerability Exposes MongoDB
Usernames and Passwords to Attackers CVE-2025-27017

Apache NiFi Vulnerability CVE-2025-27017 (NIFI-14272)

The security imperfection in Apache NiFi forms 1.13.0 through 2.2.0, where the framework incorporates MongoDB usernames and passwords in the provenance occasions created amid information handling operations.

Provenance occasions in NiFi are nitty gritty records of information ancestry that track the history of information as it moves through the system's workflow.

These occasions, implied to give straightforwardness and audibility, were inadvertently uncovering delicate confirmation data. Security analyst Robert Creese found the defenselessness and detailed it through legitimate channels.

The issue is particularly concerning since any authorised NiFi client examined to provenance occasions seems possible to see these MongoDB qualifications.

This presentation makes a critical security hazard, as compromised database accreditations may lead to unauthorised information getting to, control, or exfiltration of touchy data put away in MongoDB databases associated with the NiFi instance.

Organisations utilising influenced forms of Apache NiFi in conjunction with MongoDB confront a potential security hazard if unauthorised parties pick up and get to provenance records.

Database qualification presentation compromises the secrecy and judgment of information overseen through these frameworks. Helplessness is especially concerning for organisations directed by businesses or those caring for touchy information.

Apache has tended to resolve this issue during the most recent discharge of NiFi. Adaptation 2.3.0, unaffected by this defenselessness, appropriately evacuates accreditations from provenance occasion records.

The official proposal from the Apache NiFi group is to update form 2.3.0 to moderate this risk promptly.

For organisations incapable of updating quickly, executing strict get-to controls for provenance information and conducting security reviews to distinguish potential credential presentation are suggested as transitory measures.

Furthermore, organisations should consider turning MongoDB qualifications after overhauling to guarantee that already uncovered accreditations can no longer be utilised for unauthorised access.

This powerlessness is an update on the significance of comprehensive security reviewing over all components of information-preparing frameworks, mainly centring on how verification accreditations

are managed through the application lifecycle.

Don't forget to update and stay safe!?

Additional sources to explore: You can also search directly by CVE on Google for more information:

<https://gbhackers.com/apache-nifi-vulnerability/>

<https://securityonline.info/cve-2025-27017-apache-nifi-vulnerability-exposes-mongodb-credentials/>

<https://cybersecuritynews.com/apache-nifi-vulnerability-mongodb/>