A Vulnerability in Nx (build system) Package Could Allow for Sensitive Dat

Data: 2025-09-26 00:11:41

Autor: Inteligência Against Invaders

We recommend the following actions be taken:

* Stepsecurity.io recommends the following Immediate Remediation steps:

1. Secure organization repositories: Make any exposed organization repositories private again

- Use this query to check if your organization has been affected (replace acme with your GitHub organization name):
- https://learn.cisecurity.org/e/799323/-repositories-s-updated-o-desc/4vknyq/2542665573/h/BevE6avHam4c9BfILaqtOy_6j8sxhFFUHSx9bpBfGGw

2. Isolate affected users: Disconnect affected user(s) from the organization while mitigating this issue

3. Revoke all access tokens for affected users: In each affected user’s account settings, revoke:

- All installed apps
- All authorized apps
- All OAuth tokens (especially GitHub CLI tokens)
- All SSH keys
- All GPG keys

4. Remove forked repositories: Delete any forked repositories from affected user accounts that may contain sensitive organizational data

5. Follow comprehensive remediation: Complete all steps outlined in our remediation section to ensure no credentials remain exposed

* Apply appropriate updates provided by Nx or other vendors which use this software to vulnerable systems immediately after appropriate testing. (M1051: Update Software)

- Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
- Safeguard 7.2: Establish and Maintain a Remediation Process: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
- Safeguard 7.4: Perform Automated Application Patch Management: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- Safeguard 7.5 : Perform Automated Vulnerability Scans of Internal Enterprise Assets: Perform

automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.

- Safeguard 7.7: Remediate Detected Vulnerabilities: Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date: Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
- Safeguard 18.1: Establish and Maintain a Penetration Testing Program: Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
- Safeguard 18.2: Perform Periodic External Penetration Tests: Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
- Safeguard 18.3: Remediate Penetration Test Findings: Remediate penetration test findings based on the enterprise’s policy for remediation scope and prioritization.

* Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. (M1016: Vulnerability Scanning)

- Safeguard 16.1: Establish and Maintain a Secure Application Development Process: Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
- Safeguard 16.2: Establish and Maintain a Process to Accept and Address Software Vulnerabilities: Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.
- Safeguard 16.4 : Establish and Manage an Inventory of Third-Party Software Components: Establish and manage an updated inventory of third-party components used in development, often referred to as a “bill of materials,” as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that

the component is still supported.