Security Advisory

NPM Supply Chain Attack - 10.10.2025 (v1.0)

Background

On 14 September 2025, the Node Package Manager (NPM) repository experienced a supply chain attack, during which attackers conducted a highly targeted phishing campaign to compromise the account of an NPM package maintainer.

With privileged access, the attackers injected malicious code into widely used JavaScript packages, posing a risk to the broader software ecosystem. The incident disrupted several key NPM packages, including those critical to application development and cryptography.

The attack, named “Shai-Hulud”, searched affected hosts for tokens associated with cloud credentials such as *GITHUB_TOKEN*, *NPM_TOKEN*, *AWS_ACCESS_KEY_ID*, and *AWS_SECRET_ACCESS_KEY*. These credentials were then exfiltrated to a hardcoded remote endpoint, potentially allowing attackers to gain unauthorized access to downstream systems and repositories.

Axis Response

Axis has been actively monitoring the incident since the initial reports and immediately initiated precautionary measures to ensure the integrity and security of our software supply chain.

Our internal investigation, supported by our security and engineering teams, has found no evidence of compromise within Axis systems, environments, or customer data. Nevertheless, we have rotated all access tokens and relevant credentials, reviewed building pipelines and dependencies, and implemented enhanced monitoring to detect any unusual activity.

We will continue to closely monitor the situation and provide updates as additional information becomes available.