GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

2 April 2026

Advisory 127: AXIOS NPM Package – Supply Chain Compromise

Release Date: 31st March 2026
Impact: HIGH / CRITICAL
TLP: GREEN

The Department of Communications and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

On 31 March 2026, a sophisticated and pre-planned supply chain attack was carried out against Axios, one of the most widely used HTTP client libraries in the JavaScript ecosystem. With over 83 million weekly downloads, Axios is a foundational dependency across frontend frameworks, backend services, and enterprise applications worldwide.

The attack was executed by compromising the npm account of the primary Axios maintainer ("jasonsaayman") and using that access to publish two malicious versions of the package (1.14.1 and 0.30.4). These versions did not contain any malicious code within Axios itself. Instead, they silently injected a fake dependency — "plain-crypto-js@4.2.1" — which served as a cross-platform Remote Access Trojan (RAT) dropper.

This is a textbook supply chain attack: trusted infrastructure was weaponised to distribute malware to unsuspecting developers and organisations that simply ran "npm install" as part of their normal development or CI/CD workflow.

What are the systems affected?

The following versions of the Axios npm package are confirmed malicious and must not be used:

- Axios version 1.14.1
- Axios version 0.30.4
- Plain-crypto-js version 4.2.1

Platforms affected : Windows, MacOS and Linux

What does this mean?

The attack exploits npm's postinstall lifecycle hook — a legitimate npm feature that automatically runs a script when a package is installed. Because this hook fires silently during a normal "npm install", the malware executes without any user interaction or awareness.

Infection Chain

When a developer or CI/CD pipeline installs the malicious Axios version, the following sequence occurs automatically:

1. npm installs axios@1.14.1 or axios@0.30.4.
2. As part of the install, npm resolves the injected dependency plain-crypto-js@4.2.1.
3. npm's postinstall hook fires setup.js — an obfuscated Node.js dropper — automatically.
4. setup.js detects the operating system and contacts the C2 server (sfrclak.com:8000) to fetch a platform-specific RAT payload.
5. The RAT is installed and launched silently in the background.
6. The dropper then deletes all forensic evidence: removes the postinstall script and swaps in a clean package.json to avoid detection.

The infection chain applies for Windows, macOS amd linux even though the attack vector is different for specific platforms.

Read more..

Mitigation process

CERTVU recommends the following:

Step 1. Check for Malicious Axios Versions

Step 2. Check for RAT Artifacts on each platform

- macOS – Artifact Path / IOC is /Library/Caches/com.apple.act.mond

- Windows - Artifact Path / IOC is %PROGRAMDATA%\wt.exe | %PROGRAMDATA%\system.bat | Registry Run key pointing to system.bat
- Linux - Artifact Path / IOC is /tmp/ld.py

Step 3. Downgrade Axios to a safe Version
Step 4. Rotate all Credentials Immediately
Step 5. Block C2 Traffic

Safe Version:

- Downgrade from 1.14.1 to 1.14.0
- Downgrade from 0.30.4 to 0.30.3
- For Package -Plain-crypto-js ver. 4.2.1 – Remove entirely

Reference

1. https://thehackernews.com/2026/03/axios-supply-chain-attack-pushes-cross.html?fbclid=IwY2xjawQ5SzlleHRuA2FlbQIxMABicmlkETFlRDFDU0JGZGZHZVlmZkZ2c3J0YwZhcHBfaWQQMjIyMDM5MTc4ODIwMDg5MgABHiu5hF5z41FsQICu0y1do-jSltuNv8kM3ce8j8sHKaOjCSXNicKLI-B5ax4l_aem_XKk-191z3fu9lGpisDhUXQ
2. https://www.malwarebytes.com/blog/news/2026/03/axios-supply-chain-attack-chops-away-at-npm-trust
3. https://www.sophos.com/en-us/blog/axios-npm-package-compromised-to-deploy-malware
4. https://snyk.io/blog/axios-npm-package-compromised-supply-chain-attack-delivers-cross-platform/

.