An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2604011943

NCSC Advisory

Axios NPM Supply Chain Attack

1st, April 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

The NCSC have been made aware of a sophisticated supply chain attack impacting axios, the leading JavaScript HTTP client library which has over 100 million weekly downloads.

Stepsecurity have reported two versions of axios, 1.14.1 and 0.30.4, inject a dependency for plain-crypto-js@4.2.1 that is used to execute a postinstall script acting as a Remote Access Trojan (RAT) dropper targeting all major platforms macOS, Windows and Linux. [1]

This dropper contacts a command and control (C2) server to download the second stage payloads for the specific platform.

Once the payload is executed the malware deletes itself from the host and replaces its own package.json with a clean version to evade forensic detection.

Google Threat Intelligence Group (GTIG) has attributed this activity to UNC1069, a financially motivated North Korean APT group. [2]

Products Affected

Product	Version
axios	1.14.1
axios	0.30.4

Impact

When developers or automated systems install either version, the malicious code executes immediately, stealing sensitive credentials from the system (cloud access keys, database passwords, API tokens) and installing a Remote Access Trojan (RAT) that gives the attacker persistent access to the compromised machine.

If you have installed either affected version of axios, or detect any malicious artifacts, you should assume the system has been compromised and proceed with remediation actions.

The malicious code targeted Windows, macOS and Linux systems with platform-specific payloads, covering the full range of environments where axios is used.

Recommendations

The NCSC strongly recommends that organisations impacted by the supply chain attack revert to a safe known version of axios (e.g. 1.14.0 or earlier; 0.30.3 or earlier), harden their systems, block and conduct threat hunting for known IOCs found in the links below.

Please see the list of IOCs provided by StepSecurity and Google Threat Intelligence.

[1] https://www.stepsecurity.io/blog/axios-compromised-on-npm-malicious-versions-drop-remote-access-trojan

[2] https://cloud.google.com/blog/topics/threat-intelligence/north-korea-threat-actor-targets-axios-npm-package