Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

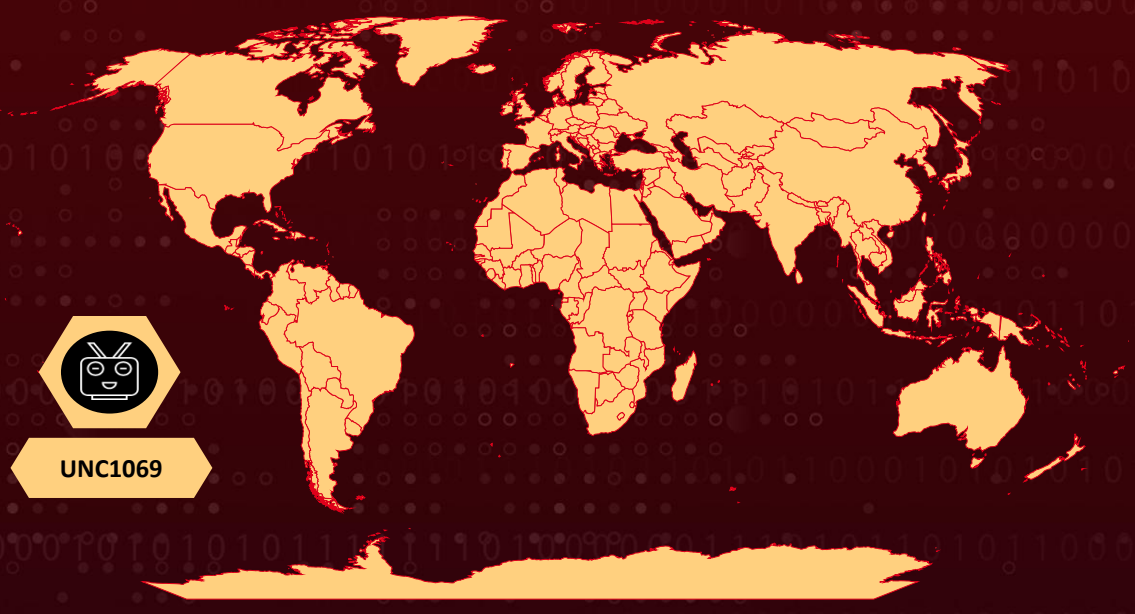
Axios npm Supply Chain Attack: What You Need to Know

Date of Publication	Admiralty Code	TA Number
April 03, 2026	A1	TA2026089

Summary

First Seen: March 30, 2026 (pre-staging); March 31, 2026 (active compromise)
Targeted Regions: Global
Targeted Platforms: Windows, macOS, Linux
Targeted Products: Axios npm package (versions 1.14.1 and 0.30.4), Node.js environments, CI/CD pipelines
Affected Users: Any developer, CI/CD pipeline, or production system that ran npm install during March 31 ~00:21–03:20 UTC and resolved, directly or transitively, to axios@1.14.1 or axios@0.30.4
Threat Actor: UNC1069 (aka BlueNorOff, APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet, TAG-71, Alluring Pisces, Selective Pisces, G0082, CryptoCore, CageyChameleon)
Malware: WAVESHAPER.V2 (aka ZshBucket RAT), SILKBELL
Attack: A North Korea-nexus threat actor compromised the npm maintainer account for the Axios JavaScript HTTP client library, one of the most widely used open-source packages with over 100 million weekly downloads, and published two poisoned versions (1.14.1 and 0.30.4) that introduced a hidden malicious dependency called plain-crypto-js. This dependency executed a cross-platform dropper during installation, which silently contacted an attacker-controlled command-and-control server and deployed platform-specific Remote Access Trojans (RATs) on Windows, macOS, and Linux systems. The malware performed credential harvesting, system reconnaissance, and established persistent backdoor access, then self-destructed to evade forensic detection.

Attack Regions



Attack Details

#1 The Axios supply chain attack (March 30–31, 2026) was a high-impact compromise of one of the most widely used JavaScript libraries in the npm ecosystem. Attackers compromised a maintainer's account using a stolen long-lived npm access token and published malicious versions (`1.14.1` and `0.30.4`). With Axios seeing ~100 million weekly downloads and present in ~80% of cloud environments, the attack created a massive blast radius during the ~3-hour exposure window.

#2 Rather than modifying Axios' core source code, the attackers introduced a malicious dependency (`plain-crypto-js`) that bypassed casual code review. It executed through npm's postinstall lifecycle hook, meaning simply installing Axios during the affected period triggered the compromise without any user interaction. A key detection indicator was the absence of OIDC (OpenID Connect) provenance metadata and SLSA (Supply-chain Levels for Software Artifacts) build attestations on the malicious releases, a departure from Axios' standard publishing workflow.

#3 Once executed, the malicious script, an obfuscated JavaScript dropper dubbed SILKBELL, contacted a C2 server at sfrclak[.]com to deploy a cross-platform RAT identified as WAVESHAPER.V2. The malware harvested developer credentials, API tokens, and cloud access keys while establishing persistent remote access. It included anti-forensic techniques such as deleting installation artifacts and restoring modified files to evade detection.

#4 The attack has been attributed to a North Korea–aligned, financially motivated threat cluster named UNC1069 (aka BlueNoroff, Sapphire Sleet, Nickel Gladstone, and Stardust Chollima) under the broader Lazarus Group. The operation demonstrated clear understanding of modern development workflows, exploiting trust in open-source packages and dependency automation.

#5 In the weeks preceding the Axios incident, another threat actor tracked as TeamPCP (UNC6780) had already launched a series of back-to-back supply chain attacks targeting open-source projects including Trivy, KICS, and LiteLLM, and the Axios compromise by UNC1069 on March 31 further intensified those existing concerns around developer ecosystem security.

#6 Affected organizations are urged to roll back to safe versions (1.14.0 or 0.30.3), rotate all exposed credentials, and enforce strict dependency pinning. This incident reinforces a critical shift in supply chain threats, attackers increasingly targeting package distribution mechanisms rather than application code itself, a pattern consistent with SolarWinds (2020), Log4j ecosystem abuse (2021), and the npm multi-package compromises of 2025.

Recommendations

Downgrade Axios to Safe Versions: Immediately roll back all Axios installations to version 1.14.0 for the 1.x branch or 0.30.3 for the 0.x legacy branch. Verify that no lockfiles (package-lock.json, yarn.lock) reference versions 1.14.1 or 0.30.4, and remove the node_modules/plain-crypto-js directory from all environments.

Pin Dependencies and Disable Auto-Upgrade: Remove caret (^) and tilde (~) version prefixes from package.json to prevent automatic resolution to malicious versions. Use overrides or resolutions blocks to force pinned versions for transitive dependencies, and disable automated dependency bots (Dependabot, Renovate) from upgrading Axios until the threat is fully mitigated.

Rotate All Exposed Secrets and Credentials: Assume all environment variables, API tokens, cloud access keys (AWS, Azure, GCP), SSH keys, database credentials, npm tokens, and CI/CD secrets present on any system where the malicious package executed have been exfiltrated. Rotate these credentials immediately from a known-clean machine and review access logs for anomalous activity.

Block C2 Infrastructure: Block all inbound and outbound traffic to the domain sfrclak.com, IP address 142.11.206.73, and port 8000 at network firewalls, DNS filters, and corporate proxies. Additionally block the related pivot domain callnrwise.com and monitor for connections to suspected related IPs 23.254.203.244 and 23.254.167.216.

Audit CI/CD Pipelines and Build Systems: Review all CI/CD pipeline logs for npm install executions between 00:21 and 03:15 UTC on March 31, 2026. Treat any persistent self-hosted runner that installed the affected versions as fully compromised. For ephemeral runners, rotate all secrets and credentials that were injected during the compromised run.

Disable npm Postinstall Scripts in Automated Builds: Use npm ci --ignore-scripts to prevent postinstall hooks from running during automated builds. Configure npm globally with npm config set ignore-scripts true in CI/CD environments to block future supply chain attacks that rely on lifecycle script execution.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
		T1195.001: Compromise Software Dependencies and Development Tools
	T1078: Valid Accounts	T1078.004: Cloud Accounts
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
		T1059.001: PowerShell
		T1059.002: AppleScript
		T1059.006: Python
		T1059.005: Visual Basic
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1070: Indicator Removal	T1070.004: File Deletion
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1027: Obfuscated Files or Information	
	T1620: Reflective Code Loading	
Discovery	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1105: Ingress Tool Transfer	
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	sfrclak[.]com, callnrwise[.]com
IPv4	142[.]11[.]206[.]73, 23[.]254[.]203[.]244, 23[.]254[.]167[.]216
URLs	Hxxp[:]//sfrclak[.]com:8000/6202033, Hxxp[:]//sfrclak[.]com:8000
SHA256	92ff08773995ebc8d55ec4b8e1a225d0d1e51efa4ef88b8849d0071230c9645a, 617b67a8e1210e4fc87c92d1d1da45a2f311c08d26e89b12307cf583c900d101, ed8560c1ac7ceb6983ba995124d5917dc1a00288912387a6389296637d5f815c, fcb81618bb15edfdedfb638b4c08a2af9cac9ecfa551af135a8402bf980375cf, e10b1fa84f1d6481625f741b69892780140d4e0e7769e7491e5f4d894c2e0e09, f7d335205b8d7b20208fb3ef93ee6dc817905dc3ae0c10a0b164f4e7d07121cd, e49c2732fb9861548208a78e72996b9c3c470b6b562576924bcc3a9fb75bf9ff, 58401c195fe0a6204b42f5f90995ece5fab74ce7c69c67a24c61a057325af668
SHA1	2553649f2322049666871cea80a5d0d6adc700ca, D6f3f62fd3b9f5432f5782b62d8cfd5247d5ee71, 07d889e2dadce6f3910dcbc253317d28ca61c766
Malicious npm Package	axios@1.14.1, axios@0.30.4, plain-crypto-js@4.2.1

TYPE	VALUE
File Paths	/Library/Caches/com.apple.act.mond, /tmp/ld.py, %PROGRAMDATA%\wt.exe, %PROGRAMDATA%\system.bat, %TEMP%\6202033.vbs, %TEMP%\6202033.ps1, HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftUpdate
Emails	ifstap@proton[.]me, nrwise@proton[.]me
Compromised npm Account	jasonsaayman
Attacker npm Account	nrwise
User-Agent	mozilla/4.0 (compatible; msie 8.0; windows nt 5.1; trident/4.0)
npm identifiers	packages.npm.org/product0, packages.npm.org/product1, packages.npm.org/product2

References

https://socket.dev/blog/axios-npm-package-compromised

https://www.sans.org/blog/axios-npm-supply-chain-compromise-malicious-packages-remote-access-trojan

https://www.wiz.io/blog/axios-npm-compromised-in-supply-chain-attack

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

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

https://www.microsoft.com/en-us/security/blog/2026/04/01/mitigating-the-axios-npm-supply-chain-compromise/

https://www.sophos.com/en-us/blog/axios-npm-package-compromised-to-deploy-malware

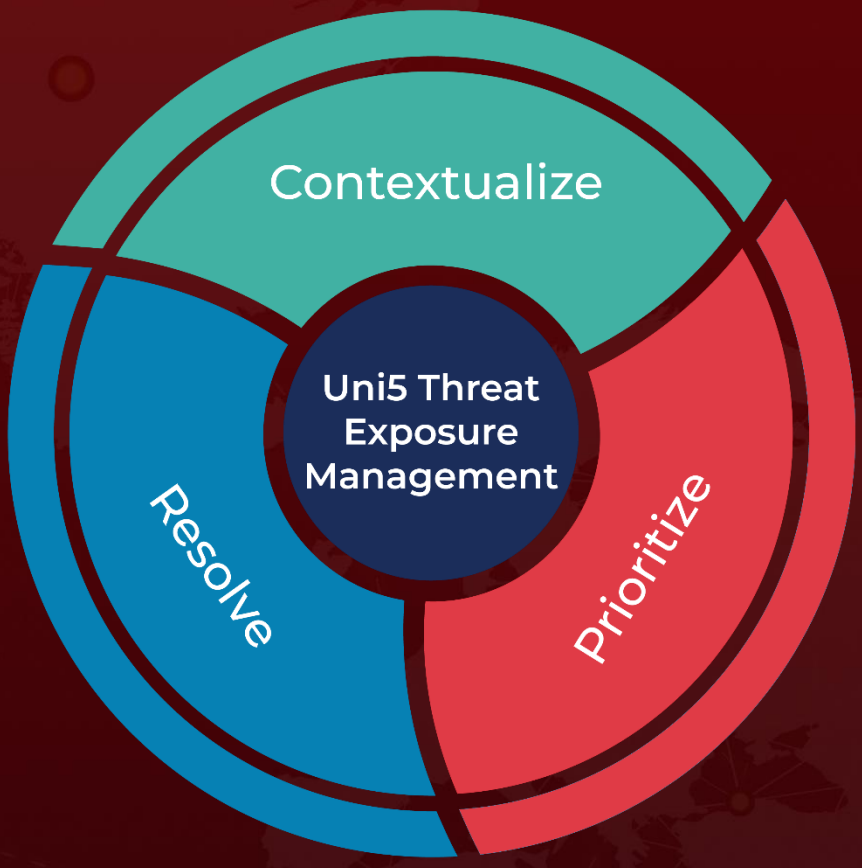
https://unit42.paloaltonetworks.com/axios-supply-chain-attack/

https://hivepro.com/threat-advisory/teampcp-automated-supply-chain-from-trivy-to-litellm-in-a-multi-ecosystem-breach/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 03, 2026 • 03:30 AM

More at www.hivepro.com