Axios npm Package Supply Chain Attack Leads to Remote Access Trojan Deployment

TL;DR

A supply chain attack impacted the Axios npm package through compromised versions axios@1.14.1 and axios@0.30.4.

These versions installed a malicious dependency that deployed a remote access trojan (RAT) across Windows, macOS, and Linux systems.

This is not tied to a CVE, and any system that installed these versions should be treated as compromised.

Overview

There is a supply chain attack impacting the Axios npm package, a widely used JavaScript HTTP client used across enterprise and development environments. Two malicious versions, axios@1.14.1 and axios@0.30.4, were published after a threat actor gained access to the maintainer's npm account.

Affected Products

- Axios npm package
  - axios@1.14.1
  - axios@0.30.4

This is not a traditional software vulnerability and does not have a CVE assigned. The core Axios code was not exploited. Instead, the attacker modified the package distribution by adding a malicious dependency, plain-crypto-js, which executed during installation.

Once installed, the malicious dependency launched a hidden script that contacted an external server and delivered a second-stage payload based on the operating system. This resulted in the installation of a remote access trojan (RAT), giving the threat actor the ability to run commands, access files, and maintain access on the system.

If this occurred within an enterprise environment, it could lead to unauthorized access to developer systems, exposure of API keys and credentials, and potential movement into other parts of the network. Because the infection occurs during a trusted installation process, it can bypass traditional detection controls and go unnoticed.

Aspire Protects

- Identify any systems that installed the affected Axios versions. **AVOID** the following versions:
  - axios@1.14.1
  - axios@0.30.4
- Remove the malicious versions and install a known safe version.
- Search for the presence of plain-crypto-js in dependencies.
- Treat impacted systems as compromised and initiate incident response procedures.
- Rotate all credentials, API keys, and tokens used on affected systems.
- Review logs for unusual outbound connections or script execution.
- Limit automatic dependency updates where possible.
- Read more about the security incident involving Axios.

TTPs to Watch

Execution

- Command and Scripting Interpreter: PowerShell [T1059.001] – The attacker may use PowerShell to run malicious scripts on Windows systems after the compromised package was installed.

Persistence

- Boot or Logon Autostart Execution [T1547] – The attacker may have maintained access by placing files on the system that continued to run after reboot.

IoCs

Malicious package versions

- axios@1.14.1
- axios@0.30.4

Suspicious dependency

- plain-crypto-js

Domain

- sfrclak[.]com

Targeted Industries

This threat impacts any organization that develops or runs JavaScript applications using npm packages, especially those with active development pipelines and automated dependency updates.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current

security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

One of the most popular JavaScript packages on earth Axios has been compromised | OpenSource Malware Blog

Axios npm Supply Chain Compromise (2026-03-31) — Full RE + Dynamic Analysis + BlueNoroff Attribution | 17 SHA256 | YARA/Sigma/Suricata rules | Live peinject validation on Daytona · GitHub

axios Compromised on npm - Malicious Versions Drop Remote Access Trojan - StepSecurity

axios - npm