مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Ongoing Supply Chain Attack – Malicious npm Package Campaign

Tracking #:432317718

Date:17-09-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed researchers uncovered a large-scale supply chain attack targeting the npm ecosystem. The attackers compromised the @ctrl/tinycolor package (2.2M weekly downloads) along with 40+ other packages across multiple maintainers.

TECHNICAL DETAILS:

A large-scale supply chain attack was uncovered targeting the npm ecosystem. The attackers compromised the @ctrl/tinycolor package (2.2M weekly downloads) along with 40+ other packages across multiple maintainers.

The malicious updates injected a bundle.js payload that:

- Downloaded and executed TruffleHog (a legitimate secret scanner).
- Searched for tokens and cloud credentials.
- Validated stolen credentials.
- Created unauthorized GitHub Actions workflows.
- Exfiltrated results to a hardcoded webhook.

This activity was attributed to the "Shai-Hulud" campaign, which has also been linked to compromises of CrowdStrike npm packages published under the crowdstrike-publisher account.

Affected Scope:

- Hundreds of npm packages confirmed compromised, including:
  - @crowdstrike: commitlint, falcon-shoelace, foundry-js, glide-core, logscale-* modules, tailwind-toucan-base
  - @ctrl, @operato, @nativescript-community, @nstudio, @things-factory, @teselagen, and many more.
- Infections observed in multiple bursts between Sept 14–16, 2025.
- Largest burst (Sept 16, 01:14 UTC) compromised nearly 100 packages in one push.

Impact:

- CI/CD compromise risk – injected workflows persist in repositories and re-trigger credential exfiltration.
- Token & credential theft – including GitHub, npm, AWS keys.
- Potential unauthorized npm publishes or code modifications.
- High likelihood of downstream impact on developers and organizations installing these packages.

Indicators of Compromise:

- bundle.js SHA-256: 46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09
- Exfiltration endpoint: hxxps://webhook[.]site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7
- de0e25a3e6c1e1e5998b306b7141b3dc4c0088da9d7bb47c1c00c91e6e4f85d6
- 81d2a004a1bca6ef87a1caf7d0e0b355ad1764238e40ff6d1b1cb77ad4f595c3
- 83a650ce44b2a9854802a7fb4c202877815274c129af49e6c2d1d5d5d55c501e
- 4b2399646573bb737c4969563303d8ee2e9ddbd1b271f1ca9e35ea78062538db
- dc67467a39b70d1cd4c1f7f7a459b35058163592f4a9e8fb4dffcbba98ef210c
- 46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09

- b74caeaa75e077c99f7d44f46daaf9796a3be43ecf24f2a1fd381844669da777

RECOMMENDATIONS:

- Uninstall / Pin – roll back to known-good versions; avoid installing recent versions of listed packages.
- Audit environments – check developer laptops, CI/CD agents, and build servers that consumed these packages.
- Rotate secrets – immediately revoke and rotate npm tokens, GitHub PATs, AWS keys, and other exposed credentials.
- Monitor activity – review logs for unusual npm publish, GitHub workflow creation, or package modifications.
- Incident response – if compromised packages were installed, treat systems as potentially breached.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://socket.dev/blog/ongoing-supply-chain-attack-targets-crowdstrike-npm-packages