

Forum:[Hack Forums](#)

Thread: [Trust Wallet links \\$8.5 million crypto theft to Shai-Hulud NPM attack](#)

MadScientist - January 5, 2026, 6:15 pm

Trust Wallet believes the compromise of its web browser to steal roughly \$8.5 million from over 2,500 crypto wallets is likely related to an "industry-wide" Sha1-Hulud attack in November.

Trust Wallet, a crypto wallet used by over 200 million people, enables users to store, send, and receive Bitcoin, Ethereum, Solana, and thousands of other cryptocurrencies and digital tokens via a web browser extension and free mobile apps.

As BleepingComputer previously reported, this December 24th incident resulted in the theft of millions of dollars in cryptocurrency from the compromised wallets of Trust Wallet users.

This happened after attackers added a malicious JavaScript file to version 2.68.0 of Trust Wallet's Chrome extension, which stole sensitive wallet data and enabled threat actors to execute unauthorized transactions.

"Our Developer GitHub secrets were exposed in the attack, which gave the attacker access to our browser extension source code and the Chrome Web Store (CWS) API key," the company said in a Tuesday update.

"The attacker obtained full CWS API access via the leaked key, allowing builds to be uploaded directly without Trust Wallet's standard release process, which requires internal approval/manual review."

As Trust Wallet explained, in the next stage of the attack, the threat actor registered the domain metrics-trustwallet.com and the subdomain api.metrics-trustwallet.com to host malicious code, which was later referenced in a trojanized version of the Trust Wallet extension.

The modified version of the official extension was built using source code obtained via exposed GitHub developer secrets, allowing the attacker to embed malicious code that collected sensitive wallet data without traditional code injection.

Using a leaked CWS key, the attacker published version 2.68 to the Chrome Web Store, which was automatically released after passing review, bypassing Trust Wallet's internal approval processes.

In response to the incident, Trust Wallet revoked all release APIs to block attempts to release new versions and ensured that the hackers couldn't steal additional wallet data by reporting the malicious domains to the NiceNIC registrar, which promptly suspended them.

Trust Wallet has also started reimbursing affected users and warned them that threat actors are currently impersonating Trust Wallet support accounts, pushing fake compensation forms, and running scams via Telegram ads.

Read More -

<https://www.bleepingcomputer.com/news/security/trust-wallet-links-85-million-crypto-theft-to-shai-hulud-npm-attack/>

Spore - January 5, 2026, 6:45 pm

isnt crypto just the bees knees. imagine getting your pockets ran for having a browser extensh

MadScientist - January 5, 2026, 7:09 pm

(Jan 5, 2026 07:45 PM)Spore Wrote: [\[CITE\]](#) isnt crypto just the bees knees. imagine getting your pockets ran for having a browser extensh

I wouldnt blame crypto for that but rather the dev team that got infected and people keeping their funds in hot wallets (say that having had my crypto hacked before as well via crypto clippers - always triple check wallet addys -_-)

Their reimbursing their users which I respect.

Hackers - January 6, 2026, 7:25 am

(Jan 5, 2026 07:45 PM)Spore Wrote: [\[CITE\]](#) isnt crypto just the bees knees. imagine getting your pockets ran for having a browser extensh

(Jan 5, 2026 08:09 PM)MadScientist Wrote: [\[CITE\]](#) I wouldnt blame crypto for that but rather the dev team that got infected and people keeping their funds in hot wallets (say that having had my crypto hacked before as well via crypto clippers - always triple check wallet addys -_-)

Their reimbursing their users which I respect.

Agreed, this isn't a crypto problem. If a bank's CI/CD is hacked, it could allow a hacker to send unauthorized wires.

People really shouldn't be using hot wallets except for when they are ready to send/receive/buy/sell.