SWISSBORG - REKT

Wednesday, September 10, 2025

Swissborg (/?tag=Swissborg) - Kiln (/?tag=Kiln) - Third-Party Dependency Risk (/?tag=Third-Party+Dependency+Risk)

read this article also in:

SwissBorg (https://x.com/swissborg) just learned that trusted partners can turn into $41.5 million headaches faster than you can spell API compromise.

The Swiss wealth management platform watched $41.5 million in SOL vanish through Kiln's backdoor (https://swissborg.com/blog/joint-statement-kiln-x-swissborg-regarding-sol-incident) - their trusted staking partner who somehow handed withdrawal keys to hackers like room service delivering towels to the wrong guest.

Eight days of patient preparation, 192.6K SOL drained in minutes, and suddenly SwissBorg's "institutional-grade custody" looked about as secure as a diary with a broken lock.

The platform scrambled to reassure users that only their SOL Earn program got gutted - affecting just 1% of customers while the other 99% watched nervously from the

sidelines.

SwissBorg promised full reimbursement from their treasury, because nothing says "we've got this under control" quite like paying millions out of pocket for someone else's security failure.

But here's the million-dollar question that's really worth $41.5 million: when your partner's API becomes your users' liability, who's actually running the security show?

Credit: Swissborg (https://swissborg.com/blog/joint-statement-kiln-x-swissborg-regarding-sol-incident), ZachXBT (https://t.me/investigations/272), Kiln (https://www.kiln.fi/post/sol-incident-swissborg---announcement), Cyrus SwissBorg (https://x.com/Cyrus_Fazel/status/1965284154402111623), CoinTelegraph (https://cointelegraph.com/news/swissborg-hacked-41m-sol-api-compromise)

September 8th, SwissBorg's Monday was about to turn into a nightmare.

ZachXBT dropped the bomb in his Telegram channel (https://t.me/investigations/272) before SwissBorg even knew they'd been hit: "SwissBorg experienced an incident a few hours ago and 192.6K SOL ($41.5M) was stolen on Solana."

No fluff, no corporate doublespeak - just the theft address that mattered.

Attacker's Address:
TYFWG3hvvxWMs2KXEk8cDuJCsXEyKs65eeqpD9P4mK1 (https://solscan.io/account/TYFWG3hvvxWMs2KXEk8cDuJCsXEyKs65eeqpD9P4mK1)

While SwissBorg's crisis team was probably still figuring out how to spell "contained incident," the blockchain had already told everyone exactly what happened and where the money went.

ZachXBT's detective work made SwissBorg's damage control look like they were playing catch-up to their own disaster.

SwissBorg surfaced 15 minutes later (https://x.com/swissborg/status/1965119220347535465) with their official statement - complete with checkmarks and reassuring bullet points about how everything else was totally fine.

"A partner API (Kiln) was compromised," they explained. "SOL Earn Program (~193k SOL, <1% of users)," they quantified. "SwissBorg app remains fully secure," they promised.

Translation: we outsourced our security to someone else, and they got owned.

When your Monday morning starts with ZachXBT announcing your $41.5 million problem to the world, how exactly do you spin that into a contained incident?

THE PARTNER PROBLEM

SwissBorg (https://x.com/swissborg) had a trust problem - they trusted Kiln (https://x.com/Kiln_finance).

Kiln finally broke silence with their own damage control masterpiece (https://www.kiln.fi/post/sol-incident-swissborg---announcement): "unauthorized access to a wallet used for staking operations" and promises that their "incident response plan" had contained the activity.

Contained where, exactly? The blockchain had already contained $41.5 million in the attacker's address hours earlier.

CEO Cyrus SwissBorg called it (https://x.com/Cyrus_Fazel/status/1965284154402111623) an "an external DeFi wallet held with a counterparty." Kiln called it (https://www.kiln.fi/post/sol-incident-swissborg---announcement) "unauthorized access." Neither wanted to say the word everyone was thinking: hack.

There's something fitting about the name though.

A kiln is a furnace (https://www.merriam-webster.com/dictionary/kiln) - once you fire clay, the shape hardens forever, cracks and all.

SwissBorg put their faith in Kiln to harden their staking infrastructure. Instead, that furnace cooked their security brittle, exposing every flaw.

The attackers didn't crack SwissBorg's vaults or exploit their smart contracts.

They compromised Kiln's API (https://cointelegraph.com/news/swissborg-hacked-41m-sol-api-compromise) - the digital bridge connecting SwissBorg's funds to Solana's staking network.

Eight days before the heist, an unstaking transaction (https://solscan.io/tx/5DCPDEVrnVdM4jHgxYGtuuzvSubg15sSpkBCxexfuApRAfXEmNfokiTyj6bxE52QNGVbPnwm9L3YzcEoMHHEpLV) that looked completely routine actually contained a nasty surprise.

While deactivating 975.33 SOL worth roughly $200k, the same transaction secretly included eight separate authorization instructions that transferred withdrawal authority from SwissBorg's legitimate controllers to "SwissBorg Exploiter 1" across multiple stake accounts.

The transaction appeared to be standard unstaking operations - the kind that happen hundreds of times daily across Solana.

But buried in those routine instructions was the skeleton key that would unlock $41.5 million eight days later.

Skeleton Key Transaction: 5DCPDEVrnVdM4jHgxYGtuuzvSubg15sSpkBCxexfuApRAfXEmNfokiTyj6bxE52QNGVbPnwm9L3YzcEoMHHEpLV (https://solscan.io/tx/5DCPDEVrnVdM4jHgxYGtuuzvSubg15sSpkBCxexfuApRAfXEmNfokiTyj6bxE52QNGVbPnwm9L3YzcEoMHHEpLV)

Blockchain security researcher Chaofan Shou called it "Bybit hack V2" (https://x.com/shoucccc/status/1965126091334713838) - and the comparison fits.

Just like Bybit's attackers hid malicious control transfers inside legitimate-looking UI transactions, SwissBorg's thieves buried their authority grab inside what appeared to be normal unstaking operations.

Kiln's statement read like corporate Mad Libs - generic crisis management boiler-

plate designed not to spook institutional clients while $41.5 million walked out the back door.

When your partner's furnace burns down your security instead of hardening it, who's really getting fired?

FOLLOW THE STOLEN LOOT

Eight days of patience, then chaos in minutes.

September 8th, 9:00 AM UTC. The thieves finally activated their skeleton key, draining 192,600 SOL faster than SwissBorg could spell incident response.

The stolen funds landed in this wallet address that Solscan now helpfully labels "SwissBorg Exploiter 1."

SwissBorg Exploiter 1:
TYFWG3hvvxWMs2KXEk8cDuJCsXEyKs65eeqpD9P4mK1 (https://solscan.io/account/TYFWG3hvvxWMs2KXEk8cDuJCsXEyKs65eeqpD9P4mK1)

But these weren't amateur hour thieves looking to dump everything on the nearest DEX.

They split their strategy into two distinct operations.

The attacker moved 189,524 SOL ($40.7 million) in one massive transfer to another wallet, where it's been sitting untouched ever since.

Transaction:
5Es6C4oT2SDXaE86P2KUCAJVfdRvfSv8oEMvtJtwsatJcFJ75BxYh4SbjBMEca6voKkc8Pc2Ja1wNE7CHmf3mUx5 (https://solscan.io/tx/5Es6C4oT2SDXaE86P2KUCAJVfdRvfSv8oEMvtJtwsatJcFJ75BxYh4SbjBMEca6voKkc8Pc2Ja1wNE7CHmf3mUx5)

Most of the stolen funds are here ($40,7 million):
2dmoNLgfP1UjqM9ZxtTqWY1YJMHJdXnUkwTrcLhL7Xoq (https://solscan.io/account/2dmoNLgfP1UjqM9ZxtTqWY1YJMHJdXnUkwTrcLhL7Xoq)

Meanwhile, a much smaller 1,000 SOL started its own journey through a chain of wallet-hopping from the original exploiter address.

SwissBorg Exploiter 1:
TYFWG3hvvxWMs2KXEk8cDuJCsXEyKs65eeqpD9P4mK1 (https://solscan.io/account/TYFWG3hvvxWMs2KXEk8cDuJCsXEyKs65eeqpD9P4mK1)

Multiple transfers across multiple addresses, with funds continuing to split and move in an endless shell game - the kind of movement pattern that screams "professional money laundering operation."

The big pile stays put while the small batch tests the waters.

Smart risk management from people who understand that moving $40 million at once is a great way to attract every blockchain investigator on the planet.

PeckShield eventually caught them testing exchange waters (https://x.com/

PeckShieldAlert/status/1965252025392005185) with a 100 SOL deposit to Bitget - but the path to get there revealed just how methodical these thieves really were. What looked like a simple exchange test was actually a carefully orchestrated relay race through multiple wallets.

First, SwissBorg Exploiter 1 sent 1,000 SOL to a second wallet they controlled.

Transaction: 2mk89MFQuqnd7dvSyM17QeeDemKmpXeL3hDroBZ6LWrvWMRyYU7RZY4k8tZ55Eg2qAEj2K3qGxBbKYntsHezf2Uk (https://solscan.io/tx/2mk89MFQuqnd7dvSyM17QeeDemKmpXeL3hDroBZ6LWrvWMRyYU7RZY4k8tZ55Eg2qAEj2K3qGxBbKYntsHezf2Uk)

SwissBorg Exploiter 2: 6bnSQH4UtGKgo4hUXRj8MeMz2bqPP6hxSaRrBjL96QaT (https://solscan.io/account/6bnSQH4UtGKgo4hUXRj8MeMz2bqPP6hxSaRrBjL96QaT)

Then Exploiter 2 sent 100 SOL to yet another address - probably testing if this intermediate wallet would get flagged.

Transaction: 32mNq9xgWf8gjWutB8k9KRjYGoxddRRN1pY9FWtk4feRVn5sTnomvFF94i4qMNNbBBzCF8BjmbP1Pe8TCg9qg6zG (https://solscan.io/tx/32mNq9xgWf8gjWutB8k9KRjYGoxddRRN1pY9FWtk4feRVn5sTnomvFF94i4qMNNbBBzCF8BjmbP1Pe8TCg9qg6zG)

Intermediate wallet: 91XrHcYL9eAFB3G7w53X4mXV4zaaZypVe3MrPCyU43dR (https://solscan.io/account/91XrHcYL9eAFB3G7w53X4mXV4zaaZypVe3MrPCyU43dR)

Finally, that intermediate wallet sent 99.98 SOL to Bitget - the deposit PeckShield caught.

Bitget Deposit Transaction: 26q2ZhRqaj4jq5LtGV1ZgHd5mVc49SSwnxKbUxjuhxBJucor3DA4bJrJjwYz42aWcbaQZ7HD73YBdm77BiJ4jNLf (https://solscan.io/tx/26q2ZhRqaj4jq5LtGV1ZgHd5mVc49SSwnxKbUxjuhxBJucor3DA4bJrJjwYz42aWcbaQZ7HD73YBdm77BiJ4jNLf)

Three hops just to test a centralized exchange with stolen funds. These weren't just professional thieves - they were paranoid professional thieves.

When your thieves show better operational discipline than your security team, what does that say about who's really running a professional operation?

WE GOT HACKED FIRE DRILL

SwissBorg's CEO Cyrus Fazel jumped into crisis mode faster than the hackers had jumped into his staking pool.

"**SwissBorg community will not take a loss,**" **he declared on X (https://x.com/Cyrus_Fazel/status/1965284154402111623), promising that "any gap in recovered funds would be covered."**

Translation: we're eating a $41.5 million bill to keep our customers happy.

The damage control playbook was textbook corporate crisis management: emphasize

that it wasn't really their fault, stress that only a tiny percentage of users were affected, and promise full compensation while the lawyers figure out who's actually liable.

"This was not a breach of the SwissBorg platform," Fazel insisted (https://x.com/Cyrus_Fazel/status/1965284154402111623). "It was an exploit that occurred on an external DeFi wallet held with a counterparty."

Sure, but that "counterparty" was handling withdrawal keys for $41.5 million of customer funds. When you outsource security, you're still outsourcing risk to your users' wallets.

SwissBorg immediately deployed the usual post-hack cavalry: white-hat hackers and security partners (https://x.com/swissborg/status/1965119220347535465) to recover compromised funds, while thanking blockchain investigators and security firms (https://x.com/Cyrus_Fazel/status/1965284154402111623) for their collaboration in tracking down funds that were probably already being split into untraceable fragments.

The platform paused Solana staking transactions (https://swissborg.com/blog/joint-statement-kiln-x-swissborg-regarding-sol-incident) while highlighting that the (https://x.com/swissborg/status/1965123506477359471) "SwissBorg app remains fully secure and all other funds in Earn programs are 100% safe."

Because nothing inspires confidence quite like selective service shutdowns after a massive theft.

Kiln, meanwhile, went full lockdown mode, disabling their dashboard, widget, and APIs (https://status.kiln.fi/incidents/01K4MQS2ARNE55B2KP97HCPR8Z) until they could figure out how hackers had turned their infrastructure into a $41.5 million withdrawal service.

When your partner's response is 'turn everything off until we figure out what happened,' how exactly does that qualify as professional partnership?

SwissBorg survived their $41.5 million Monday, but the bill came with more than just treasury depletion.

Eight days of patience, one skeleton key transaction, and suddenly "institutional-grade custody" looked about as trustworthy as a house of cards in a hurricane.

The Swiss platform learned the hard way that your security is only as strong as your weakest API endpoint - and that endpoint belonged to someone else.

Kiln got to keep their "enterprise-grade staking" marketing while SwissBorg got to keep the $41.5 million invoice.

The thieves got to keep most of their SOL sitting in digital storage, probably laughing at how a few authorization instructions buried in routine unstaking operations had unlocked institutional treasure.

Users got their promise of full compensation, but promises don't erase the fundamental problem: when you trust partners to handle withdrawal keys, you're not running a custody service - you're running a very expensive trust exercise.

The blockchain never lies, but the people building on top of it sure know how to spin a good story about "contained incidents" and "external counterparties."

SwissBorg will rebuild, Kiln will patch their systems, and the crypto world will move on to the next spectacular failure of operational security masquerading as institutional innovation.

If crypto was built to eliminate trusted third parties, why do we keep handing our keys to the exact institutions that prove they don't deserve them?

donate (ETH / ERC20): 0x3C5c2F4bCeC51a36494682f91Dbc6cA7c63B514C (https://etherscan.io/address/0x3C5c2F4bCeC51a36494682f91Dbc6cA7c63B514C)