

Analysis of xSushi's incident

eboado

Nov 2021

TLDR

1. A theoretically possible but financially non-profitable attack vector using xSUSHI on V2 was detected on 27/10/2021
2. Members of the Aave and other DeFi communities worked together to avoid any attack on the protocol
3. A proposal to completely eliminate the attack surface was created and executed by the Aave community on day 02/11/2021
4. No attack was ever performed and the funds remained safe during the whole process
5. I propose a bounty for 2 DeFi community members for their selfless contribution

Introduction

From 27/10/2021 to 02/11/2021, after a vulnerability was exploited on the Cream protocol, a public alarm was raised on the Aave ecosystem, with people claiming a similar potential vulnerability affecting Aave v2.

As summary, a potential attack vector affecting Aave v2 and xSUSHI was found, precautionary measures were taken and finally no attack was executed.

This post is an attempt from my side, as developer member of the Aave community to give a more complete version of what happened and what not, obviously from my own subjectivity, but as somebody that was involved in all the different phases.

Timeline

Time (UTC)	Event
27/10/2021 2pm	Cream incident
27/10/2021 6pm to 8pm	Members of the Aave community, the Aave Genesis team and other groups like Gauntlet start evaluating potential attack scenarios on Aave. In parallel, other individuals start also checking different liquidity protocols potentially vulnerable to similar type of attacks
Skip to main content 10pm	First evaluation by Aave community members and Gauntlet shows that, under certain circumstances, xSUSHI could be used to perform an attack on the

Time (UTC)	Event
	Aave V2 market. At the same time, it becomes clear that the liquidity conditions are not met to perform the attack. First step to be proposed to Aave governance is decided to be disabling xSUSHI as borrowing asset on v2 and, as precautionary measure due to its similar nature, freezing of LP assets on the AMM market. Gauntlet starts working on the proposal
28/10/2021 4pm	@flashfish0x from the Yearn community and @nipun_pit from Alpha Finance reach out to @stani to first, alert about the potential problem with xSUSHI and second, help with simulations of the attack's feasibility. A War room is created, initially with @flashfish0x , @nipun_pit , members of the Aave Genesis team and members of the Aave community
28/10/2021 4pm - onwards	Ongoing discussion on the War Room about the attack scenarios and their feasibility, involving technical and economical aspects. Members of the Sushi community, Gauntlet and members of the Yearn community are added to the War Room. The situation is stable, as no attack can be performed, but the liquidity conditions were met in the past and could be met again in the future (even if at that moment unrealistic), so it becomes clear that the proposal in progress is needed. Gauntlet progresses with the writing of the proposal to disable xSUSHI and freezing the LP assets, together with members of the Aave community and the Genesis team
29/10/2021 ~00.30am	The Proposal is submitted to Aave Governance voting
29/10/2021 ~12am	After discussion with @Andyko @emilio , I contact Chainlink as oracle provider for the Aave protocol, to initiate brainstorming for a permanent solution for the pricing of xSUSHI
29/10/2021 ~18pm	Pre-communication from the Aave Genesis account about the work-in-progress, informing Aave users that no funds are at risk at the moment here
29/10/2021 ~18pm - 01/11/2021 ~00.30am	Continuous monitoring of the situation in terms of liquidity movements and progress on research with Chainlink for the final solution to enable again xSUSHI and the rest of assets
01/11/2021 ~00.30am	Queueing of the proposal on time-lock
02/11/2021 ~00.30am	Execution of the proposal. There is no attack scenario anymore and no attack was performed

Analysis

xSUSHI is a governance token representing a stake position on the Sushi platform: holders of SUSHI token can deposit it on the SushiBar facility, in return for voting rights on Sushi and a model of rewards built on top.

[Skip to main content](#)

From a technical perspective, xSUSHI is what is denominated as a “wrapped” version of SUSHI, as people deposit X amount of SUSHI and receive Y amount of xSUSHI, with the value of the last going up continuously via an exchange rate.

In what concerns Aave, as of February 10th, the Sushi community proposed xSUSHI to be listed on Aave V2, proposal that passed with really good support [here](#) . The listing of the asset was both as deposit/borrow asset and collateral, with really conservative initial parameters that later on were modified.

As with any other asset on Aave, one of the most fundamental aspects of their listing is the pricing model. Usually with what can be considered “simple” tokens (not involving any wrapping or any other more advance technical/economic) the pricing is as simple as connecting a Chainlink price feed to the protocol for that asset, getting a rate ASSET/ETH or ASSET/USD to do the calculations.

But in the case of “complex” assets like xSUSHI, the pricing method is a bit different. As the stake/withdraw of SUSHI from xSUSHI can be done without any type of constraint, it is safe to assume that the price of xSUSHI derives from the price of the underlying SUSHI, which at the moment is more liquid and, consequently, a better assumption for the Aave protocol.

The implementation of the previous model can be found on [this adapter smart contract](#) , which main function is the one providing the price here:

```
function latestAnswer() external view override returns (int256) {
    uint256 exchangeRate = (IERC20(SUSHI).balanceOf(xSUSHI).mul(1ether))
    uint256 sushiPrice = uint256(IExtendedAggregator(SUSHI_ORACLE).latestAnswer());
    return int256(sushiPrice.mul(exchangeRate).div(1 ether));
}
```

As it is possible to see, the calculation is simple: an exchange rate between SUSHI and xSUSHI is calculated based on the balance of SUSHI “deposited” on the xSUSHI contract and the xSUSHI total supply; then that exchange rate is multiplied by the price of SUSHI/ETH provided by a Chainlink price feed.

Now, going back to Cream’s attack vector, the fundamental (and quite original compared with previous attacks) levers there were:

1. Contraction of the supply of a “complex” token, to be able to have a bigger impact on its later price manipulation.
2. Injection of capital of the underlying token on the “complex” one (referred usually as [Skip to main content](#) to increase considerably its value, as a small supply of the “complex” token will represent big amount of underlying.

Taking into account that, for us was natural to check all “complex” assets listed on Aave and their pricing algorithm, to try to understand if they were vulnerable to similar vectors as Cream's. And pretty soon, it was clear that xSUSHI could potentially be.

A high-level attack vector would be:

1. Same as on the Cream's case, an attacker owns 2 wallet addresses: wallet A and B
2. With B, the attacker does a flash loan of a big amount of capital that can be used as collateral in Aave, with as high LTV as possible. For example WETH or stable coins like DAI or USDC are good candidates. Let's assume WETH from now on
3. Once the WETH collateral is deposited on B, the attacker initiates a cycle of:
 - 3.1. Borrow the maximum allowed xSUSHI against the WETH
 - 3.2. Send the borrowed xSUSHI to A and deposit it there
 - 3.3. Borrow with B more xSUSHI, which A made available by depositing
 - 3.4. Repeat until the LTV limit on B
4. On the last “cycle” between B and A, the last borrowed amount of xSUSHI by B is not re-deposited back by A, as it will be used for the next phase of the attack
5. The situation at this point is that B has a big amount of WETH collateral and big amount of xSUSHI debt, while A has only a big amount of xSUSHI deposited and some amount of xSUSHI (from the previous point), with the sum of both being equal to the debt of B
6. Now it's necessary to “contract” the supply of xSUSHI, one of the main levers of the attack. For that, the attacker takes the xSUSHI left not deposited on A and burns it on the SushiBar, withdrawing SUSHI and at the same time reducing the supply. In addition, to maximise the “contraction” the attacker tries to flash-loan or borrow in any way more xSUSHI available in the market to do the same. The current scenario is that ideally for the attacker, now the supply of xSUSHI is really low
7. Now, as we commented before, the formula to calculate the price of xSUSHI of Aave involves an exchange rate which is in high-level equal to the balance of SUSHI on xSUSHI divided by the xSUSHI supply. The supply on the denominator at the moment is really low, so to increase the final result, it is necessary to increase the balance of SUSHI on xSUSHI. For this, the attacker takes all the SUSHI received from the withdrawals on the previous steps, plus tries to get as much SUSHI as possible from the market, and then “injects” this SUSHI on xSUSHI, the second attack's lever
8. At the moment, the situation of A and B on Aave didn't change, but the price of xSUSHI is way higher, ideally for the attacker, multiple times up. The consequences of this on A and B are:

[Skip to main content](#)

- A has xSUSHI deposited, which after the price increase has really big value, artificial, inflated. This can be used to borrow a big amount of available assets, way more than it should be possible
- B is on a situation of liquidation, as it has a big debt of xSUSHI (which price was inflated) which value is way higher than the WETH collateral

9. So at this point, the attacker borrows as much as possible with A as to: cover all funds he used to execute the attack (WETH flash-loaned to deposit as collateral in B, borrowed xSUSHI to “contract” and borrowed SUSHI to “inflate”) and take profit

10. Once the attack is executed, the situation for the protocol concerning A and B is:

10.1. A most probably borrowed all the funds available on Aave, but the collateral value is way lower than it should, so A is deeply “underwater”, so the protocol is under-collateralized

10.2. B just gets abandoned, as it is not profitable for attacker, with only potential to further profit via liquidation of the position

As explained before, this type of attack or other variations of the same were not possible to execute after Cream's incident, even if actually the liquidity conditions made them possible at some previous points of time. These liquidity conditions are the following:

- Enough xSUSHI should be available in the Aave market (or other liquidity protocols with capability to borrow from) to contract the supply on 6). The amounts available from 27/10 to 02/11 were not really close to make the attack feasible, but one of the precautionary measures was to try to contact axSUSHI holders for them to withdraw from the protocol
- Enough SUSHI should be available in the market to “inflate” the price on 9). Considering the granularity of SUSHI holders and SUSHI presence on facilities where borrowing from is considerably more difficult (or impossible given the usage), the attacker should have acquired in the order of multiple hundreds on million USD. Another precautionary measure was to try to contact all parties with important SUSHI holdings to monitor for potential liquidity movements

Extra important facts important on the attack are:

- xSUSHI had in general more influence on the attack than SUSHI, because the potential was doubled: affecting the contraction of the supply via withdrawal, and affecting the “inflation” phase by injecting the capital just withdrawn. This was actually something good, as the liquidity conditions for xSUSHI were pretty difficult to achieve by a single actor in short amount of time
- Flash-loan capital available for attacks is factually almost (or without almost) unlimited. This was expected since the introduction of flash-loans first on Aave v1, but right now the order of magnitude an attacker can mobilise is all the time in the order of billions USD, with no upper threshold in several vectors

[Skip to main content](#)

Finally, after the the proposal executed on 02/11, the protocol was fully protected again and no attack was performed on the Aave protocol.

Still, this should act as a reminder on how the introduction of new assets on Aave or any other DeFi protocol incurs always risk; risk that like in this case can become factual with attack scenarios that even contributors of protocol don't really know.

For this particular case, the steps forward are the further development and research around new pricing systems for assets of complex nature as xSUSHI, together with deeper due diligence on all listing steps of new assets.

Conclusion

As a member of the Aave community and directly involved during the whole process, I would like to highlight specially the work on research of the potential attack vector by [@flashfish0x](#) and [@nipun_pit](#) . Even if the attack scenario was already detected by members of the Aave community before, I believe their selfless contribution deserves a bounty and, taking into account the likelihood of the vector, **I propose a bounty of \$50k each**.

In addition, again as a member of the Aave community, I would like to thank for the involvement of [@mudit_gupta](#) , [@0xgasper](#) and [0xmaki](#) from the Sushi community, the whole [Gauntlet team](#) , [@bantg](#) from the Yearn community and [@stani](#) , [@emilio](#) , [@Andyko](#) , [@herskindlasse](#) and [@Zer0dots](#) from the Aave community.

Last but not least, a personal reflection. During Cream's incident and this one described, I observed unfortunate public communications and miss-behaviours from members of DeFi communities, included this Aave one I proudly belong to. Looking in perspective, it is quite ridiculous given the amount of things we share on this ecosystem versus the ones that separate us. I hope that in the future, it will not be only on these kind of situations where all communities work together in a fully collaborative way.

Thanks again to everybody involved

Ernesto

[🔗 ARC - Enable Borrowing of DPI on Aave Markets](#)

[🔗 Gauntlet Update: V3 Markets Integration Progress](#)

[🔗 Aave Grants DAO Update and Renewal](#)

[🔗 ARC: Q2 Dynamic Risk Parameters](#)

[🔗 BGD. Swap of price feed of xSUSHI on Aave v2 Ethereum](#)

fig

Nov 2021

[Skip to main content](#) taking the time to summarize a complex incident.

A bounty for the community members work and selflessness seems fair and deserving.

I also believe rewarding users from other communities is a great way to incentivize more frequent cross-protocol participation. Cheers @flashfish0x, @nipun_pit - well done.

A quick question about your last line:

eboado:

I observed unfortunate public communications and miss-behaviours from members of DeFi communities, included this Aave one I proudly belong to

How do we deter this behavior from happening in the future? Does it require funding for additional human capital such as a communication lead, or is it values based?

eboado

Nov 2021

fig:

How do we deter this behavior from happening in the future? Does it require funding for additional human capital such as a communication lead, or is it values based?

I believe it is the last. The Aave community always characterise itself for being really welcoming and collaborative with all others, so it is up to each member to keep those high standards at all time. For me, it is pretty clear there is a lot to lose not following that path always.

kx9x

Nov 2021

How was the \$50,000 amount determined?

Here is the bug bounty page for reference:

[Aave – Open Source DeFi Protocol | Bug Bounty](#)

Unless there is sufficient proof that it wasn't almost certain to be exploitable in the future, then a \$250,000 bounty seems to align with the published amounts.

Also, cheers to those involved. Great to see success stories where exploitable angles have been patched before they can be used.

Emilio

Nov 2021

The bug bounty request is a way to thank the security researchers and contributors that were the first to be involved outside the Aave community. Although they provided useful insights that further


[Skip to main content](#) n that the attack was only theoretically possible but not economically

feasible, the Aave community members and gauntlet had already identified the issue, determined the attack was not feasible through simulations, and started developing a fix before they actually joined. The simulations were incomplete though, that's where they helped with great additional information.

eboado**Nov 2021**

As you point out [@kx9x](#) , partially that bug bounty page was used as reference for the bounty, but it is important to note that the community should actually work updating the bug bounty program, as the current market size is considerably larger than when the current one was defined. That being said, the bounty is actually \$100k between the 2 security researches, and as [@Emilio](#) pointed out, technically it was not a disclosure because as I commented in the post, there were parties of this community (me included) aware of the problem before they contact. As much as I appreciate their contribution, it would be unfair to give a really big bounty (this one is not precisely small) if it was not a disclosure.

Related Topics

Topic	Replies	Views	Activity
 Aave v2/v3 security incident 04/11/2023	139	21.4k	Nov 2023
AIP-44 Discussion	16	3.3k	Nov 2021
[ARC] Price Manipulation Implications on Aave: October 2022	16	4.8k	Dec 2022
[TEMP CHECK] Safety Module Upgrade Part II - Asset Diversity, SM Categories & Slashing Updates	4	2.5k	May 2023
ARC - Enable Borrowing of DPI on Aave Markets	1	1.9k	Jan 2022