# Claim Investigation Report

Reporter：InsurAce.io Date：2023/11/06

## A. About this Document

This document presents the investigation and findings regarding the claim request submitted to InsurAce.io conducted and evaluated by the InsurAce.io Advisory Board.

## B. Claim Request Details

*This section presents the claim request details submitted by the applicant.*

| | |
|---|---|
| **Claim ID** | # 84 (Polygon) |
| **Claim Time** | 2023/08/29 23:01:50 |
| **Protocol** | Exactly Protocol |
| **Loss Event Time** | 2023/08/18 |
| **Loss Amount** | 132,051.0000 USDC |
| **Claim Amount** | 132,051.0000 USDC |

**Claim Description Submitted by the Applicant**

On August 18 2023, Exact.ly was exploited with around 7.3m$ loss on Optimism.

https://twitter.com/BlockSecTeam/status/1692533205109547202

https://twitter.com/ExactlyProtocol/status/1692950170705518879

We had ETH and wstETH on the protocol, and suffered a loss of 132051$.

Our address (0x54240c950ff793a4eb5895a56f859216cb1c3f0d) was impacted in 3 transactions :

block 108375561
https://optimistic.etherscan.io/tx/0xe8999fb57684856d637504f1f0082b69a3f7b34dd4e7597bea376c9466813585

block 108375565
https://optimistic.etherscan.io/tx/0xbe1bf0b97ed6bd1e9a95227db05dbb9da9f4218ec8c93c485b5d58d90ddeb169

block 108375566
https://optimistic.etherscan.io/tx/0x0a9002ad9306be7d9a9223866fd3a3040bc04882a745780df53a02e85ee9b872

Before hack, at block 108375560 (2023-08-18 09:11:37 UTC)

We had 262.8289 ETH supplied and 187.7738 ETH borrowed, so a 75,0551 ETH net supply.

We also had 196.8586 wstETH suppplied and 135.2682 wstETH borrowed, so a net supply of 61.5904 wstETH.

After hack, at block 108375567 (2023-08-18 09:11:51 UTC)

We had 0 ETH supplied and 0 ETH borrowed

We had 131.1405 wstETH supplied and 72.8282 wstETH borrowed, so a net supply of 58,3123 wstETH.

Total loss: 75,0551 ETH (125781$ according to 2023/08/18 coingecko average) and 3.2781 wstETH (6270$).

We are sending at claims@insurace.io a snapshot of our address on block 108375560 and 108375567 and the python code used to obtain it.

## C. Cover Details

*This section presents the policy details purchased by the applicant.*

| | |
|---|---|
| **Risk Type** | Smart Contract Vulnerability |
| **Protocol** | Exactly Protocol |
| **Cover Period** | 2023/07/24 - 2023/09/22 |
| **Cover Amount** | 207,000 USDC |
| **Cover T&C** | Smart Contract Vulnerability Cover Wording |

## D. Investigation and Findings

*This section presents the investigation and root cause analysis conducted by the Advisory Board.*

**Incident Description and Root Cause Analysis**

### Summary of the Incident

**Exactly Protocol suffered a security breach where:**

- Date: 09:10 – 09:53 UTC, August 18, 2023
- Loss Amount: $7.6 million
- Root cause: vulnerabilities within the DebtManager peripheral contract — a feature designed to help users leverage and deleverage positions in Exactly Protocol's Markets.

**Details of the Exploit:**

Two different attackers exploited the vulnerability:

- 0x3747DbBCb5C07786a4c59883E473A2e38F571af9: main attacker that was able to extract ~4330 ETH.
- 0x0000000002088951336D7972746a135F2956417 (tiffa.eth): copycat attacker that started to replicate the original hack approximately 3 hours later. Extracted ~140 ETH.

**Account Losses Analysis**

The Exactly team disclosed an

Official Losses Per Account Disclosure

(https://docs.google.com/spreadsheets/d/1kZCGUnwhN6rXHZjPZrzayzZPHUmm1L_hypvpRGcqdO0/edit#gid=1635590080 )

Where the covered wallet address lies in, as shown below:

| | Account | WETH | USDC | wstETH | OP | Total in $ | % of Total | % Cumulative |
|---|---|---|---|---|---|---|---|---|
| 1 | 0xf35e261393f9705e10b378c6785582b2a5a71094 | | 1,773,834.57 | | | $1,773,834.57 | 23.30% | 23.30% |
| 2 | 0xf6da9e9d73d7893223578d32a95d6d7de5522767 | 1,022.57 | | | | $1,689,292.30 | 22.19% | 45.50% |
| 3 | 0x3cf3c6a96357e26de5c6f8be745dc453aad59249 | 7.36 | 531,781.90 | | | $543,942.07 | 7.15% | 52.64% |
| 4 | 0x87bf260aef0efd0ab046417ba290f69ae24c1642 | | 518,170.38 | | | $518,170.38 | 6.81% | 59.45% |
| 5 | 0x2f0d2701b620b639e44e1824446a0d63d7a05c31 | | 472,158.47 | | | $472,158.47 | 6.20% | 65.65% |
| 6 | 0x551cfb91acd97572ba1c2b177eeb667c207ce759 | | 430,280.97 | | | $430,280.97 | 5.65% | 71.30% |
| 7 | 0x8789e0a45b270d7fd9aed1a72682f6530a722c50 | | 326,718.35 | | | $326,718.35 | 4.29% | 75.60% |
| 8 | 0xd1adb83cd6390c6bbd619fdd79fc37f9f58f1a4c | | 300,509.26 | | | $300,509.26 | 3.95% | 79.54% |
| 9 | 0x166ed9f7a56053c7c4e77cb0c91a9e46bbc5e8b0 | 118.76 | | | | $196,184.28 | 2.58% | 82.12% |
| 10 | 0x516e5b72c3fd2d2e59835c82005ba6a2bc5788a4 | | 168,784.83 | | | $168,784.83 | 2.22% | 84.34% |
| 11 | 0xaf935695eb156b6fe95af0e83daafbd62ca37af5 | | 163,931.37 | | | $163,931.37 | 2.15% | 86.49% |
| 12 | 0x316be293c8f2380769e7b7e7382679fe5a3b6600 | 95.54 | | | | $157,838.12 | 2.07% | 88.57% |
| 13 | 0x54240c950ff793a4eb5895a56f859216cb1c3f0d | 75.06 | | 3.28 | | $130,252.28 | 1.71% | 90.28% |
| 14 | 0x654f1c992758b0dd491e3ac67f084cacf98aa77c | 52.88 | | | | $87,357.73 | 1.15% | 91.42% |
| 15 | 0xe72185a9f4ce3500d6dc7ccdcfc64cf66d823be8 | 34.34 | 672.46 | | | $57,394.18 | 0.75% | 92.18% |
| 16 | 0x055a0495104aea25551e7a58eba88dc56709e871 | | 54,600.83 | | | $54,600.83 | 0.72% | 92.90% |
| 17 | 0x6d74e589b0adb2b1941e91d8cda35ddb7b15f4ff | 29.97 | | | | $49,512.10 | 0.65% | 93.55% |

**For more information:**

https://twitter.com/phalcon_xyz/status/1692477201655189722?s=46&t=cyu_GujhD4g8_5KKh1-M9w

https://medium.com/@exactly_protocol/exactly-protocol-incident-post-mortem-b4293d97e3ed

## Post Solutions of Exactly Protocol

- August 21th: Unpaused the protocol( https://twitter.com/ExactlyProtocol/status/1693053785692664206 )
- August 22nd : Attempted to contact with hackers and recover the funds with $700K reward (https://twitter.com/ExactlyProtocol/status/1693756962708631950 )
- August 30th : Released post mortem report (https://medium.com/@exactly_protocol/exactly-protocol-incident-post-mortem-b4293d97e3ed )
- Sep 16th : Failed to get in touch with the hackers, and after that the Exactly team initiate an investigation with the United States Department of Homeland Security (DHS), with case number NY02HR23NY0001. (https://twitter.com/ExactlyProtocol/status/1707856082339508235 )
- Sep 27th : Announced that the DebtManager peripheral contract was audited by @ABDKconsulting (https://twitter.com/ExactlyProtocol/status/1706790377716338807 )
- Sep 27th : Reopened the Web App Strategies Section (https://medium.com/@exactly_protocol/the-web-app-strategies-section-is-back-51bf622d77e9 )
- Oct 28th : Released the Recap Q3 2023 Report and stated that the Exactly team is collaborating with Chainalysis and other security experts to identify

the attackers and take appropriate measures. (https://medium.com/@exactly_protocol/exactly-protocol-recap-4-e58db6dca618 )

- Nov 6th: A compensation proposal "[EXAIP-03] Addressing the Exactly Protocol Hack and Compensating Affected Users" was submitted by community member to address the Exactly protocol hack and the voting process started. https://twitter.com/exactlyprotocol/status/1721528870120063414?s=46
- Nov 10th: The compensation proposal "[EXAIP-03] Addressing the Exactly Protocol Hack and Compensating Affected Users" passed the voting process and will be implemented. https://twitter.com/ExactlyProtocol/status/1722716452984123633

## The Communication from Claimant

Proof of loss from the claimant:

```
CallWeb3FunctionByBlock % python3 main.py
At Block : 108375560 (2023-08-18 09:11:37+00:00)
Wallet address : 0x54240C950fF793A4eB5895a56F859216cB1c3f0D
Coingecko average USD price (for 1 ETH) :  1675.8621709457839
Coingecko average USD price (for 1 wstETH) : 1912.958689792414
--------------------------------------------------------------------------------
Contract address : 0xc4d4500326981eacD020e20A81b1c479c161c7EF (exaWETH)

Supply amount : 260.76000340559982549 exaWETH
--------- raw : 260760003405599825490
Converted amount : 262.828918475060254178 WETH
--------- raw : 262828918475060254178

Borrow amount : 187.773771330992879683 WETH
--------- raw : 187773771330992879683

Rate : 1 exaWETH = 1.007934173348825775 WETH
Diff : 75.055147144067374495 WETH
--------------------------------------------------------------------------------
Contract address : 0x22ab31Cd55130435b5efBf9224b6a9d5EC36533F (exawstETH)

Supply amount : 196.831388306796125759 exawstETH
--------- raw : 196831388306796125759
Converted amount : 196.858699453142316698 wstETH
--------- raw : 196858699453142316698

Borrow amount : 135.268260794820125543 wstETH
--------- raw : 135268260794820125543

Rate : 1 exawstETH = 1.000138754019778703 wstETH
Diff : 61.590438658322191155 wstETH
--------------------------------------------------------------------------------
```

Over the past two months following a security incident, the team at InsurAce has been in continuous communication with the Exactly team, awaiting their solutions.

Concurrently, the InsurAce team has engaged with the claimant for the investigation of the claim, and for conveying the latest updates on the situation.

The claimant has affirmed that "if the DHS is successful in recovering the funds of Exactly (or Exactly paying a compensation plan), you (the InsurAce platform) and only you (the InsurAce platform) will be reimbursed". This statement will be duly incorporated and attached in our claim assessment and investigation report.

**Actual Loss Amount**

The official loss amount for this covered wallet address (0x54240c950ff793a4eb5895a56f859216cb1c3f0d) from Exactly Protocol's loss analysis is 75.055147 WETH and 3.278103 wstETH.

Based on the above investigation findings and proof of loss provided by the Claimant, the actual loss amount is:

| Asset Impacted | Amount Impacted | Daily Average Market Price ($) | Actual Loss Amount ($) |
|---|---|---|---|
| WETH | 75.055147 | 1,675.862 | 125,782.082 |
| wstETH | 3.278103 | 1,912.958 | 6,270.876 |
| **Total Asset Impacted** | | | **132,052.957** |

**For more information:**

- Loss per account analysis: https://docs.google.com/spreadsheets/d/1kZCGUnwhN6rXHZjPZrzayzZPHUmm1L_hypvpRGcqdO0/edit#gid=1635590080
- Smart Contract Vulnerability Cover Wording: https://docs.insurace.io/landing-page/documentation/cover-products/smart-contract-vulnerability-cover

**Actual Loss Event Time**

2023/08/18

**Others**

## E. Conclusion

*This section presents the reference conclusion on claim acceptance as proposed by the Advisory Board.*

| | |
|---|---|
| **Claim Advice** | The Advisory Board have considered these reports, as well as feedback from experts across the industry and the recommended course of action is: **Claimable** |
| **Remarks** | |

- On August 18, 2023, Exactly Protocol encountered a security incident between 09:10 – 09:53 UTC, leading to a $7.6 million loss, caused by a vulnerability in the DebtManager peripheral contract. Two attackers exploited this weakness, with the primary attacker extracting about 4330 ETH and a copycat extracting around 140 ETH.
- The claimant's loss is due to unauthorized, malicious, or criminal attacks, hacks or exploits of any malfunction or programming flaw in the Designated

Smart Contract during the Cover Period (Smart Contract Vulnerability Cover Wordings, Clause 2.1(d)(i))

- On November 16, 2023, a compensation plan was proposed by the community with one million EXA tokens to be distributed to the 117 affected users following a vesting schedule spanning 48 months. The proposal passed the voting process on November 10, 2023.

## F. Payout Proposal

### Compensable Amount Summary

Based on the Smart Contract Vulnerability Cover Wording and according to a discussion between InsurAce and the Cover Owner, InsurAce will provide a payout to the Cover Owner amounting to 90% of the verified loss, while acknowledging and accepting any compensation token issued by the protocol in response to the hack event.

**Summary:**

Total Asset Impacted: $132,052.96

Expected Payout Amount: 90% * $132,052.96 = **$118,847.66**

- If this payout proposal is accepted: The payout following the amount in the table above will be made accordingly.
- If this payout proposal is rejected: All claims submitted related to this attack will be rejected without compensation.