



verichains

SECURITY AUDIT OF
AVT PLATFORM



Public Report

Jun 20, 2023

Verichains Lab

info@verichains.io

<https://www.verichains.io>

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Ethereum	An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications.
Ether (ETH)	A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network.
Smart contract	A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
Solidity	A contract-oriented, high-level language for implementing smart contracts for the Ethereum platform.
Solc	A compiler for Solidity.
Optimism	The Optimism protocol is a Layer2 protocol that is intended to help Ethereum users speed up and pay less fees for transactions made on the Ethereum network.

Report for AVT

Security Audit – AVT Platform

Version: 1.0 – Public Report

Date: Jun 20, 2023



EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Jun 20, 2023. We would like to thank the AVT Team for trusting Verichains Lab in auditing smart contracts. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the AVT Platform. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team found some vulnerabilities in the application.



TABLE OF CONTENTS

1. MANAGEMENT SUMMARY	5
1.1. About AVT Platform	5
1.2. Audit scope.....	5
1.3. Audit methodology	5
1.4. Disclaimer	6
2. AUDIT RESULT	7
2.1. Overview	7
2.2. Findings.....	7
2.2.1. Incorrect ALP referral reward increasing MEDIUM	7
2.2.2. Outdated version of base GMX smart contracts HIGH.....	8
2.2.3. Incorrect check during trader referral code update in ReferralStorage LOW	9
2.3. Additional notes and recommendations	10
2.3.1. Use modifier instead of private view to validate handler	10
3. VERSION HISTORY	11

1. MANAGEMENT SUMMARY

1.1. About AVT Platform

AVT is a decentralised, transparent and non custodial perpetual platform built on Optimism where users can swap, long or short BTC, ETH and OP with up to 50x leverage.

1.2. Audit scope

The AVT Platform smart contracts was based on a version of GMX smart contracts on commit [aa34bafd9a52f14af4b82484ec0286f4d5564fb9](https://github.com/gmx-io/gmx-contracts/tree/aa34bafd9a52f14af4b82484ec0286f4d5564fb9) (<https://github.com/gmx-io/gmx-contracts/tree/aa34bafd9a52f14af4b82484ec0286f4d5564fb9>).

This audit focused on identifying security flaws in the design and implementation of the modified AVT smart contracts compared to the original GMX smart contracts.

It was conducted on commit [17ebf5ea371d62d12b6d567b40a37e29b894683f](https://github.com/vhuarui/mw-avt-contracts/tree/17ebf5ea371d62d12b6d567b40a37e29b894683f) on AVT contracts repo (<https://github.com/vhuarui/mw-avt-contracts/tree/17ebf5ea371d62d12b6d567b40a37e29b894683f>).

1.3. Audit methodology

Our security audit process for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using public and RK87, our in-house smart contract security analysis tool.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that were considered during the audit of the smart contract:

- Integer Overflow and Underflow
- Timestamp Dependence
- Race Conditions
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert
- DoS with Block Gas Limit
- Gas Usage, Gas Limit and Loops
- Redundant fallback function
- Unsafe type Inference
- Reentrancy
- Explicit visibility of functions state variables (external, internal, private and public)

- Logic Flaws

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the contract functioning; creates a critical risk to the contract; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the contract with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 1. Severity levels

1.4. Disclaimer

Please note that security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a 100% secure smart contract. However, auditing allows discovering vulnerabilities that were unobserved, overlooked during development and areas where additional security measures are necessary.

2. AUDIT RESULT

2.1. Overview

The AVT Platform smart contracts (as well as original GMX smart contracts) was written in `Solidity` language. The code base also imported several contracts from OpenZeppelin's public library.

2.2. Findings

During the audit process, the audit team found some vulnerabilities in the given version of AVT Platform.

AVT Team fixed some issues, according to Verichains's draft report in commit [645ceb940fa6acd10e8b1c7514ae4ab1979049f0](#).

#	Issue	Severity	Status
1	Incorrect ALP referral reward increasing	MEDIUM	Fixed
2	Outdated version of base GMX smart contracts	HIGH	Acknowledged
3	Incorrect check during trader referral code update in <code>ReferralStorage</code>	LOW	Acknowledged

2.2.1. Incorrect ALP referral reward increasing MEDIUM

Affected files:

- `contracts/staking/RewardRouterV2.sol`

Current implementation of `handleRewards` function:

```
275 function handleRewards(  
276       
277       
278       
279       
280       
281       
282       
283       
284       
285       
286       
287       
288       
289       
290       
291       
292       
293       
294       
295       
296       
297       
298       
299       
300       
301       
302       
303       
304       
305       
306       
307       
308       
309       
310       
311       
312       
313       
314       
315       
316       
317       
318       
319       
320       
321       
322       
323       
324       
325       
326       
327       
328       
329       
330       
331       
332       
333       
334       
335       
336       
337       
338       
339       
340       
341       
342       
343       
344       
345       
346       
347       
348       
349       
350       
351       
352       
353       
354       
355       
356       
357       
358       
359       
360       
361       
362       
363       
364       
365       
366       
367       
368       
369       
370       
371       
372       
373       
374       
375       
376       
377       
378       
379       
380       
381       
382       
383       
384       
385       
386       
387       
388       
389       
390       
391       
392       
393       
394       
395       
396       
397       
398       
399       
400       
401       
402       
403       
404       
405       
406       
407       
408       
409       
410       
411       
412       
413       
414       
415       
416       
417       
418       
419       
420       
421       
422       
423       
424       
425       
426       
427       
428       
429       
430       
431       
432       
433       
434       
435       
436       
437       
438       
439       
440       
441       
442       
443       
444       
445       
446       
447       
448       
449       
450       
451       
452       
453       
454       
455       
456       
457       
458       
459       
460       
461       
462       
463       
464       
465       
466       
467       
468       
469       
470       
471       
472       
473       
474       
475       
476       
477       
478       
479       
480       
481       
482       
483       
484       
485       
486       
487       
488       
489       
490       
491       
492       
493       
494       
495       
496       
497       
498       
499       
500       
501       
502       
503       
504       
505       
506       
507       
508       
509       
510       
511       
512       
513       
514       
515       
516       
517       
518       
519       
520       
521       
522       
523       
524       
525       
526       
527       
528       
529       
530       
531       
532       
533       
534       
535       
536       
537       
538       
539       
540       
541       
542       
543       
544       
545       
546       
547       
548       
549       
550       
551       
552       
553       
554       
555       
556       
557       
558       
559       
560       
561       
562       
563       
564       
565       
566       
567       
568       
569       
570       
571       
572       
573       
574       
575       
576       
577       
578       
579       
580       
581       
582       
583       
584       
585       
586       
587       
588       
589       
590       
591       
592       
593       
594       
595       
596       
597       
598       
599       
600       
601       
602       
603       
604       
605       
606       
607       
608       
609       
610       
611       
612       
613       
614       
615       
616       
617       
618       
619       
620       
621       
622       
623       
624       
625       
626       
627       
628       
629       
630       
631       
632       
633       
634       
635       
636       
637       
638       
639       
640       
641       
642       
643       
644       
645       
646       
647       
648       
649       
650       
651       
652       
653       
654       
655       
656       
657       
658       
659       
660       
661       
662       
663       
664       
665       
666       
667       
668       
669       
670       
671       
672       
673       
674       
675       
676       
677       
678       
679       
680       
681       
682       
683       
684       
685       
686       
687       
688       
689       
690       
691       
692       
693       
694       
695       
696       
697       
698       
699       
700       
701       
702       
703       
704       
705       
706       
707       
708       
709       
710       
711       
712       
713       
714       
715       
716       
717       
718       
719       
720       
721       
722       
723       
724       
725       
726       
727       
728       
729       
730       
731       
732       
733       
734       
735       
736       
737       
738       
739       
740       
741       
742       
743       
744       
745       
746       
747       
748       
749       
750       
751       
752       
753       
754       
755       
756       
757       
758       
759       
760       
761       
762       
763       
764       
765       
766       
767       
768       
769       
770       
771       
772       
773       
774       
775       
776       
777       
778       
779       
780       
781       
782       
783       
784       
785       
786       
787       
788       
789       
790       
791       
792       
793       
794       
795       
796       
797       
798       
799       
800       
801       
802       
803       
804       
805       
806       
807       
808       
809       
810       
811       
812       
813       
814       
815       
816       
817       
818       
819       
820       
821       
822       
823       
824       
825       
826       
827       
828       
829       
830       
831       
832       
833       
834       
835       
836       
837       
838       
839       
840       
841       
842       
843       
844       
845       
846       
847       
848       
849       
850       
851       
852       
853       
854       
855       
856       
857       
858       
859       
860       
861       
862       
863       
864       
865       
866       
867       
868       
869       
870       
871       
872       
873       
874       
875       
876       
877       
878       
879       
880       
881       
882       
883       
884       
885       
886       
887       
888       
889       
890       
891       
892       
893       
894       
895       
896       
897       
898       
899       
900       
901       
902       
903       
904       
905       
906       
907       
908       
909       
910       
911       
912       
913       
914       
915       
916       
917       
918       
919       
920       
921       
922       
923       
924       
925       
926       
927       
928       
929       
930       
931       
932       
933       
934       
935       
936       
937       
938       
939       
940       
941       
942       
943       
944       
945       
946       
947       
948       
949       
950       
951       
952       
953       
954       
955       
956       
957       
958       
959       
960       
961       
962       
963       
964       
965       
966       
967       
968       
969       
970       
971       
972       
973       
974       
975       
976       
977       
978       
979       
980       
981       
982       
983       
984       
985       
986       
987       
988       
989       
990       
991       
992       
993       
994       
995       
996       
997       
998       
999       
1000      
1001      
1002      
1003      
1004      
1005      
1006      
1007      
1008      
1009      
1010      
1011      
1012      
1013      
1014      
1015      
1016      
1017      
1018      
1019      
1020      
1021      
1022      
1023      
1024      
1025      
1026      
1027      
1028      
1029      
1030      
1031      
1032      
1033      
1034      
1035      
1036      
1037      
1038      
1039      
1040      
1041      
1042      
1043      
1044      
1045      
1046      
1047      
1048      
1049      
1050      
1051      
1052      
1053      
1054      
1055      
1056      
1057      
1058      
1059      
1060      
1061      
1062      
1063      
1064      
1065      
1066      
1067      
1068      
1069      
1070      
1071      
1072      
1073      
1074      
1075      
1076      
1077      
1078      
1079      
1080      
1081      
1082      
1083      
1084      
1085      
1086      
1087      
1088      
1089      
1090      
1091      
1092      
1093      
1094      
1095      
1096      
1097      
1098      
1099      
1100      
1101      
1102      
1103      
1104      
1105      
1106      
1107      
1108      
1109      
1110      
1111      
1112      
1113      
1114      
1115      
1116      
1117      
1118      
1119      
1120      
1121      
1122      
1123      
1124      
1125      
1126      
1127      
1128      
1129      
1130      
1131      
1132      
1133      
1134      
1135      
1136      
1137      
1138      
1139      
1140      
1141      
1142      
1143      
1144      
1145      
1146      
1147      
1148      
1149      
1150      
1151      
1152      
1153      
1154      
1155      
1156      
1157      
1158      
1159      
1160      
1161      
1162      
1163      
1164      
1165      
1166      
1167      
1168      
1169      
1170      
1171      
1172      
1173      
1174      
1175      
1176      
1177      
1178      
1179      
1180      
1181      
1182      
1183      
1184      
1185      
1186      
1187      
1188      
1189      
1190      
1191      
1192      
1193      
1194      
1195      
1196      
1197      
1198      
1199      
1200      
1201      
1202      
1203      
1204      
1205      
1206      
1207      
1208      
1209      
1210      
1211      
1212      
1213      
1214      
1215      
1216      
1217      
1218      
1219      
1220      
1221      
1222      
1223      
1224      
1225      
1226      
1227      
1228      
1229      
1230      
1231      
1232      
1233      
1234      
1235      
1236      
1237      
1238      
1239      
1240      
1241      
1242      
1243      
1244      
1245      
1246      
1247      
1248      
1249      
1250      
1251      
1252      
1253      
1254      
1255      
1256      
1257      
1258      
1259      
1260      
1261      
1262      
1263      
1264      
1265      
1266      
1267      
1268      
1269      
1270      
1271      
1272      
1273      
1274      
1275      
1276      
1277      
1278      
1279      
1280      
1281      
1282      
1283      
1284      
1285      
1286      
1287      
1288      
1289      
1290      
1291      
1292      
1293      
1294      
1295      
1296      
1297      
1298      
1299      
1300      
1301      
1302      
1303      
1304      
1305      
1306      
1307      
1308      
1309      
1310      
1311      
1312      
1313      
1314      
1315      
1316      
1317      
1318      
1319      
1320      
1321      
1322      
1323      
1324      
1325      
1326      
1327      
1328      
1329      
1330      
1331      
1332      
1333      
1334      
1335      
1336      
1337      
1338      
1339      
1340      
1341      
1342      
1343      
1344      
1345      
1346      
1347      
1348      
1349      
1350      
1351      
1352      
1353      
1354      
1355      
1356      
1357      
1358      
1359      
1360      
1361      
1362      
1363      
1364      
1365      
1366      
1367      
1368      
1369      
1370      
1371      
1372      
1373      
1374      
1375      
1376      
1377      
1378      
1379      
1380      
1381      
1382      
1383      
1384      
1385      
1386      
1387      
1388      
1389      
1390      
1391      
1392      
1393      
1394      
1395      
1396      
1397      
1398      
1399      
1400      
1401      
1402      
1403      
1404      
1405      
1406      
1407      
1408      
1409      
1410      
1411      
1412      
1413      
1414      
1415      
1416      
1417      
1418      
1419      
1420      
1421      
1422      
1423      
1424      
1425      
1426      
1427      
1428      
1429      
1430      
1431      
1432      
1433      
1434      
1435      
1436      
1437      
1438      
1439      
1440      
1441      
1442      
1443      
1444      
1445      
1446      
1447      
1448      
1449      
1450      
1451      
1452      
1453      
1454      
1455      
1456      
1457      
1458      
1459      
1460      
1461      
1462      
1463      
1464      
1465      
1466      
1467      
1468      
1469      
1470      
1471      
1472      
1473      
1474      
1475      
1476      
1477      
1478      
1479      
1480      
1481      
1482      
1483      
1484      
1485      
1486      
1487      
1488      
1489      
1490      
1491      
1492      
1493      
1494      
1495      
1496      
1497      
1498      
1499      
1500      
1501      
1502      
1503      
1504      
1505      
1506      
1507      
1508      
1509      
1510      
1511      
1512      
1513      
1514      
1515      
1516      
1517      
1518      
1519      
1520      
1521      
1522      
1523      
1524      
1525      
1526      
1527      
1528      
1529      
1530      
1531      
1532      
1533      
1534      
1535      
1536      
1537      
1538      
1539      
1540      
1541      
1542      
1543      
1544      
1545      
1546      
1547      
1548      
1549      
1550      
1551      
1552      
1553      
1554      
1555      
1556      
1557      
1558      
1559      
1560      
1561      
1562      
1563      
1564      
1565      
1566      
1567      
1568      
1569      
1570      
1571      
1572      
1573      
1574      
1575      
1576      
1577      
1578      
1579      
1580      
1581      
1582      
1583      
1584      
1585      
1586      
1587      
1588      
1589      
1590      
1591      
1592      
1593      
1594      
1595      
1596      
1597      
1598      
1599      
1600      
1601      
1602      
1603      
1604      
1605      
1606      
1607      
1608      
1609      
1610      
1611      
1612      
1613      
1614      
1615      
1616      
1617      
1618      
1619      
1620      
1621      
1622      
1623      
1624      
1625      
1626      
1627      
1628      
1629      
1630      
1631      
1632      
1633      
1634      
1635      
1636      
1637      
1638      
1639      
1640      
1641      
1642      
1643      
1644      
1645      
1646      
1647      
1648      
1649      
1650      
1651      
1652      
1653      
1654      
1655      
1656      
1657      
1658      
1659      
1660      
1661      
1662      
1663      
1664      
1665      
1666      
1667      
1668      
1669      
1670      
1671      
1672      
1673      
1674      
1675      
1676      
1677      
1678      
1679      
1680      
1681      
1682      
1683      
1684      
1685      
1686      
1687      
1688      
1689      
1690      
1691      
1692      
1693      
1694      
1695      
1696      
1697      
1698      
1699      
1700      
1701      
1702      
1703      
1704      
1705      
1706      
1707      
1708      
1709      
1710      
1711      
1712      
1713      
1714      
1715      
1716      
1717      
1718      
1719      
1720      
1721      
1722      
1723      
1724      
1725      
1726      
1727      
1728      
1729      
1730      
1731      
1732      
1733      
1734      
1735      
1736      
1737      
1738      
1739      
1740      
1741      
1742      
1743      
1744      
1745      
1746      
1747      
1748      
1749      
1750      
1751      
1752      
1753      
1754      
1755      
1756      
1757      
1758      
1759      
1760      
1761      
1762      
1763      
1764      
1765      
1766      
1767      
1768      
1769      
1770      
1771      
1772      
1773      
1774      
1775      
1776      
1777      
1778      
1779      
1780      
1781      
1782      
1783      
1784      
1785      
1786      
1787      
1788      
1789      
1790      
1791      
1792      
1793    <
```

```
295  
296         IAlpReferralReward(alpReferralReward).increaseAlpReferral(account, avtAmount);  
297     }  
_____  
318 }
```

In this part of function, we have two rewards to claim: one for AVT staked, and one for ALP staked. The ALP staked rewards includes rewards from tracker1 and tracker2. Only the rewards from ALP staked will be used to calculate the increasing ALP referral reward.

But the current implementation code includes both AVT staked and ALP staked in reward calculation, as in the following statements:

```
292 avtAmount = avtAmount.add(avtAmount1).add(avtAmount2);  
293  
294 IAlpReferralReward(alpReferralReward).increaseAlpReferral(account, avtAmount);
```

RECOMMENDATION

Update the code to include only ALP staked rewards in the calculation, as follows:

```
289 if (_shouldClaimStakedAlpReward) {  
_____  
294     IAlpReferralReward(alpReferralReward).increaseAlpReferral(account,  
avtAmount1.add(avtAmount2));  
295 }
```

UPDATES

- *Jun 14, 2023*: This issue has been acknowledged and fixed by the AVT Team in commit [645ceb940fa6acd10e8b1c7514ae4ab1979049f0](#).

2.2.2. Outdated version of base GMX smart contracts **HIGH**

Compared to the original version on which the AVT contracts were based, the latest version of the GMX contracts includes numerous updates, including bug fixes and improvements.

- Latest version of GMX contracts (as of writing time): <https://github.com/gmx-io/gmx-contracts/tree/649a1b328725c4523530ff8fc7ca5fc2bd4167a0>
- Changes between latest version and original version: <https://github.com/gmx-io/gmx-contracts/compare/aa34bafd9a52f14af4b82484ec0286f4d5564fb9..649a1b328725c4523530ff8fc7ca5fc2bd4167a0>

For example, this is one of the bug fixes in the updated contracts:

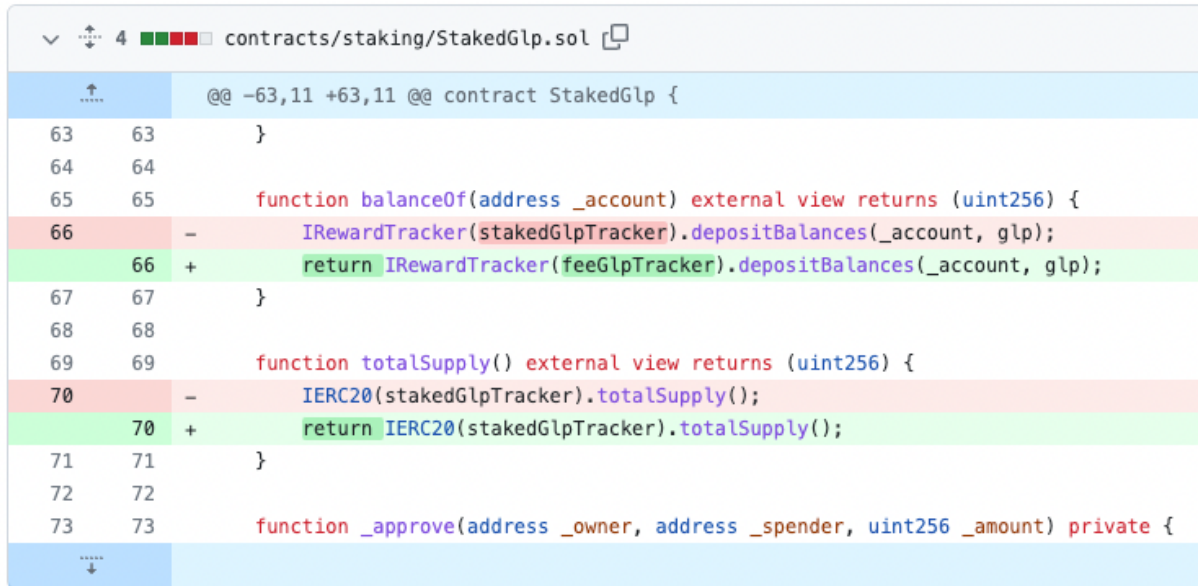


Image 1. A bug fix from updated GMX contracts

We recommend updating the AVT contracts to utilize the latest version of the GMX contracts.

UPDATES

- Jun 14, 2023: This issue has been acknowledged by the AVT Team.

2.2.3. Incorrect check during trader referral code update in ReferralStorage **LOW**

Affected files:

- contracts/referrals/ReferralStorage.sol

Current implementation of `setTraderReferralCode` function is as follow:

```
77 function setTraderReferralCode(address _account, bytes32 _code) external override
onlyHandler {
78     require(traderReferralCodes[msg.sender] == bytes32(0), "ReferralStorage: already
set");
79     _setTraderReferralCode(_account, _code);
80 }
```

Because we are updating the referral code for `_account`, not for `msg.sender`, so instead of `require(traderReferralCodes[msg.sender] == bytes32(0), ...)`; the checking statement should be `require(traderReferralCodes[_account] == bytes32(0), ...)`;

By the way, these require statements should be placed in `_setTraderReferralCode` function.

RECOMMENDATION

Move the require statements to the internal function `_setTraderReferralCode`

```
121 function _setTraderReferralCode(address _account, bytes32 _code) private {  
122     require(traderReferralCodes[_account] == bytes32(0), "ReferralStorage: already  
set");  
123     traderReferralCodes[_account] = _code;  
124     emit SetTraderReferralCode(_account, _code);  
125 }
```

UPDATES

- *Jun 14, 2023*: This issue has been acknowledged by the AVT Team.

2.3. Additional notes and recommendations

2.3.1. Use modifier instead of private view to validate handler

Contract

AlpReferralReward (contracts/staking/AlpReferralReward.sol)

To enhance handler permission validation, it is advisable to replace the usage of a private view (`_validateHandler`) with a modifier. This approach aligns with a common pattern employed in multiple instances within the AVT smart contract source codes.

```
modifier onlyHandler() {  
    require(isHandler[msg.sender], "AlpReferralReward: forbidden");  
    _;  
}
```

UPDATES

- *Jun 14, 2023*: This issue has been acknowledged by the AVT Team.

Report for AVT

Security Audit – AVT Platform

Version: 1.0 – Public Report

Date: Jun 20, 2023



3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	Jun 20, 2023	Public Report	Verichains Lab

Table 2. Report versions history