- Home
- Vulnerabilities!
- Blog
- Services
- About
- Contact

Epic Games Rocket League 1.95 (AK::MemoryMgr::GetPoolName) Stack Buffer Overrun

Title: Epic Games Rocket League 1.95 (AK::MemoryMgr::GetPoolName) Stack Buffer Overrun
Advisory ID: ZSL-2021-5651
Type: Local/Remote
Impact: System Access, DoS
Risk: (4/5)
Release Date: 30.04.2021

Summary

Rocket League is a high-powered hybrid of arcade-style soccer and vehicular mayhem with easy-to-understand controls and fluid, physics-driven competition.

Description

The game suffers from a stack-based buffer overflow vulnerability. The issue is caused due to a boundary error in the processing of a UPK format file, which can be exploited to cause a stack buffer overflow when a user crafts the file with a large array of bytes inserted in the vicinity offset after the magic header. Successful exploitation could allow execution of arbitrary code on the affected machine.

```
------------------------------------------------------------------------------

0:000> g
(3568.230c): Security check failure or stack buffer overrun - code c0000409 (!!! second chance !!!)
Subcode: 0x2 FAST_FAIL_STACK_COOKIE_CHECK_FAILURE
RocketLeague!AK::MemoryMgr::GetPoolName+0x84164:
00007ff6`4a660424 cd29 int 29h

------------------------------------------------------------------------------
```

Vendor

Epic Games Inc. - https://www.epicgames.com | https://www.rocketleague.com
Psyonix, LLC - https://www.psyonix.com

Affected Version

<=1.95

Tested On

Microsoft Windows 10

Vendor Status

[25.04.2021] Vulnerability discovered.
[26.04.2021] Vendor contacted.
[26.04.2021] Vendor responds with instructions to open a ticket at HackerOne.
[26.04.2021] ZSL creates a ticket on HackerOne, asking if this is something they can handle or is in scope.
[26.04.2021] HackerOne reviews the question.
[26.04.2021] HackerOne states that RCE due to BoF is in scope but because no PoC provided, closes the ticket.
[28.04.2021] ZSL provides PoC file.
[28.04.2021] HackerOne reopens the ticket, asking further details.
[28.04.2021] ZSL provides further details and video demonstrating the issue.
[30.04.2021] HackerOne states that folder CookedPCConsole is not writable for the Limited user. Administrator privilege is required to inject the payload, therefore, this privilege escalation scenario cannot be accepted as valid. For this scenario to be accepted as a valid RCE scenario, you must be able to inject the payload as a Limited User, and you can execute cmd.exe and demonstrate the privilege escalation scenario.
[30.04.2021] HackerOne closes the ticket and changes the status to Informative.
[30.04.2021] ZSL explains that there are insecure permissions on the folder that can allow payload injection and EoP. Further, through BoF (which is a vulnerability) code execution is possible. ZSL didn't want to provide weaponized PoC where calc.exe pops, stating that it is sufficient to confirm the issue with provided PoC UPK crash file.
[30.04.2021] Public security advisory released.

PoC

rocketleague_bof.txt
rocketleague_hats.rar

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://packetstormsecurity.com/files/162436/Epic-Games-Rocket-League-1.95-Stack-Buffer-Overrun.html
[2] https://exchange.xforce.ibmcloud.com/vulnerabilities/201129
[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32238
[4] https://nvd.nist.gov/vuln/detail/CVE-2021-32238
[5] https://ubuntu.com/security/CVE-2021-32238
[6] https://security-tracker.debian.org/tracker/CVE-2021-32238
[7] https://www.cvedetails.com/cve/CVE-2021-32238/
[8] https://vuldb.com/?id.175346
[9] https://www.exploit-db.com/exploits/49848
[10] https://cxsecurity.com/issue/WLB-2021050075
[11] https://exchange.xforce.ibmcloud.com/vulnerabilities/201456

Changelog

[30.04.2021] - Initial release
[04.05.2021] - Added reference [1] and [2]

[19.06.2021] - Added reference [3], [4], [5], [6], [7], [8], [9], [10] and [11]

Contact

Zero Science Lab

Web: https://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- ## Rete mirabilia

- ## We Suggest

- ## Profiles

- Site Meter