huntr

Session tokens are not invalidated on logout in heroiclabs/nakama

1

✓ Valid Reported on May 24th 2022

Description

The session cookie is not invalidated on logout so, it can be used after logout as well.

Proof of Concept

Login to the Nakama console.
Intercept the request. Below is a sample request:

```
GET /v2/console/user HTTP/1.1
Host: localhost:7351
Accept: application/json, text/plain, */*
Authorization: Bearer <token>
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Referer: http://localhost:7351/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Logout from the application.
Replay the request. Response is received as an authorized user.

Impact

Old session tokens can be used to authenticate to the application and send authenticated requests.

Occurrences

TS authentication.service.ts L82-L86

CVE
CVE-2022-2306
(Published)

Vulnerability Type
CWE-613: Insufficient Session Expiration

Severity
High (8.2)

Registry
Other

Affected Version
3.12.0

Visibility
Public

Status
Fixed

Found by

nerrorsec
@nerrorsec
amateur

This report was seen 678 times.

We are processing your report and will contact the **heroiclabs/nakama** team within 24 hours.
6 months ago

We have contacted a member of the **heroiclabs/nakama** team and are waiting to hear back
6 months ago

We have sent a follow up to the **heroiclabs/nakama** team. We will try again in 7 days.
6 months ago

nerrorsec modified the report 6 months ago

Chat with us

nerrorsec modified the report 6 months ago nerrorsec modified the report 6 months ago

A **heroiclabs/nakama** maintainer has acknowledged this report 6 months ago

Andrei Mihu 6 months ago Maintainer

Thanks for the report, we're looking into this and will respond in more depth as soon as possible.

Andrei Mihu validated this vulnerability 5 months ago

nerrorsec has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Andrei Mihu marked this as fixed in **3.13.0** with commit **ce8d39** 5 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

authentication.service.ts#L82-L86 has been validated ✓

Sign in to join this conversation

leaderboard

FAQ

contact us

terms

privacy policy

team

Chat with us