UNCATEGORIZED

Bug Bounty Adventures: A NodeBB 0-day

Share

March 25th, 2022

> *Opera maintains both a [public bug bounty program](), and a [private program](), where security researchers can submit security issues they have found in Opera's products for cash rewards. We like to highlight some of the issues that have been submitted, to educate the community about the types of issues they should be on the look-out for. In this post, we outline a vulnerability that was submitted to us concerning a third-party-developed software – [NodeBB]()* – which turned out to be a 0-day vulnerability.

In May 2021, we received a bug bounty submission from researcher Mar0uane, about a

In the report, Mar0uane outlined that it was possible to create a single-sign-on authorization code for his own user, then trick a different user into associating their account with that auth-code, via a Cross-Site Request (a CSRF). The following instructions to reproduce the issue were given:

1. Create two accounts; A (Attacker) and B (Victim).
2. Sign into the attacker account, and begin the process of enabling Google SSO.
3. Intercept the request, and retrieve the URI similar to: *https://forums.opera.com/auth/google/callback?code=XXXX*
4. In a new browser, logged in with the victim account, navigate to the intercepted URI.

After step #4, the victim's account is associated with the SSO account from the attacker's account – with no user interaction needed. This also means that a foreign website can embed a frame to this URI, resulting in a logged-in user (such as an administrator) unsuspectingly being compromised, without their knowledge.

This type of vulnerability is not new, nor overly complicated. OWASP outlines this type of issue, which should be standard for many pentesters. However, what is somewhat interesting about this specific vulnerability, is that NodeBB is forum software used by thousands of users around the world. For many companies – and individuals – performing such basic tests against software may be seen as a waste of time, due to the assumption that *somebody*, *somewhere*, will have already tested for this sort of vulnerability.

According to NodeBB's developer, this report was not the first they had heard about this issue. In June of 2018, it was reported via their bug bounty program. However, the same issue was accidentally re-introduced when that part of the code was refactored in early 2021. Effectively, Mar0uane had reported a 0-day that to us that had been un-fixed just five months earlier – showing the power of the bug bounty system both via the original report in June of 2018, and in May 2021.

In the end the vulnerability was fixed. While we normally don't pay-out for issues found in third-party code, an exception was made in this case, and both us and NodeBB, rewarded the reporter with some cash. Ultimately, this shows that when pentesting a website, it's worth testing your assumptions.

Joshua Rogers

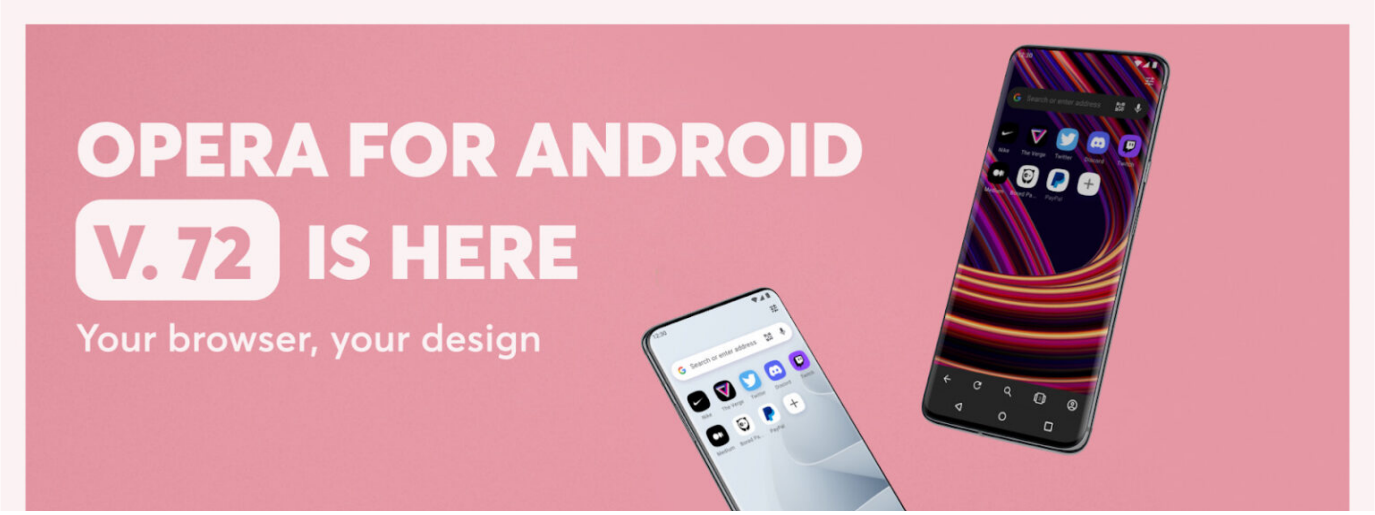
#bug bounty

User comments

Comments: 0

Start a discussion

Log in to post



SECURITY

Safe Browsing now on Opera for Android

November 11th, 2022

← →

Opera

You deserve a better browser

Opera's free VPN, Ad blocker, and Flow file sharing. Just a few of the must-have

© 1995-2022 Opera Norway

All rights reserved