Background

On April, 7 we received a security report on the Immunefi platform which hosts theMakerDAO bug bounty program. The whitehat hacker demonstrated it was possible to force a blank page to be stored into the CDN cache for a given URL in the Governance Portal, which could lead to some or all of the Governance Portal pages being inaccessible by the users, depending of the extent to which the vulnerability could have been exploited.

Actions taken

Upon receiving the report we started a root cause analysis between TechOps and Jetstream, with the goal of better understanding the attack vector and potential mitigation steps.

During the investigation phase we found that the vulnerability was unusual in nature, given that we were unable to find documentation on similar cases. It also proved difficult to assess whether the root cause was related to the frontend application code or its hosting infrastructure configuration such as CDN provider. As a result it took us longer than usual to identify a root cause, despite back-and-forth with the whitehat hacker. Given that no user and protocol funds were at risk and the whitehat hacker was willing to collaborate, we took over a week to find consensus on mitigation steps and implement them accordingly. The process involved multiple internal escalations, outreach to various software/infra vendors, testing various fixes and discussion with the whitehat hacker.

On April 19th we marked the vulnerability report as valid, but did contest the ‘critical severity’ label. Immunefi’s mediation team ended up investigating the report and related discourse, with the outcome of the report being indeed of critical severity.

Improvements implemented

Jetstream implemented several improvements to enhance application (Governance Portal) security, particularly related to headers. One enhancement involved modifying the middleware to ensure that only request headers are returned in the NextResponse.next.request object. This adjustment streamlines header management, improving efficiency and reducing potential vulnerabilities. Additionally, Jetstream refined the response headers by removing request headers from them entirely. Now, the response headers solely contain the Content Security Policy (CSP).

TechOps implemented a worker (specific software) for the infrastructure that rewrites and removes unnecessary headers from all requests coming to specific endpoints thus making it impossible to bring down the Governance Portal sending corrupted requests.

This change has been implemented for all MakerDAO websites and subdomains that are managed and controlled by TechOps Services EA.

Planned improvements

In addition to the fixes that have already been implemented, there are a couple of improvements that we agreed to make. They are mainly related to the process of reporting, escalating and trying to avoid bottlenecks whenever high priority bug issues are reported:

1. Improve the inbound process of the bug bounty program through a more granular definition of system component stewards.

2. Automate notification and alerting process, facilitating fast response.

3. Narrow the scope of ‘critical’ web application bugs by improving its definition as part of the bug bounty program terms.

4. More granularly define what’s considered out-of-scope for the bug bounty program.

Closing

Based on the above we authorize@psychonaut (as steward of the bug bounty program) to proceed with the bounty payout.

Thanks to @jetstream-ea and @techops-services-ea teams for collaborating on the issues and making it possible to resolve it in a proper manner.