Web Cache Poisoning Vulnerability Report for Figma

Vulnerability Summary:

A potential Web Cache Poisoning vulnerability has been identified in the HTTP response for a request to the Figma storefront. Web Cache Poisoning occurs when an attacker manipulates cached responses to deliver malicious content to users, exploiting how cache servers store responses. The issue arises when cache servers do not appropriately handle user input or headers, potentially allowing malicious actors to alter the cached data.

Vulnerability Details:

Vulnerability Type: Web Cache Poisoning

Affected URL: https://store.figma.com/products/gestures-longsleeve

Vulnerable Component: Shopify CDN response for product pages.

Risk: High

Attackers could modify cached responses to include malicious code or redirects.

Users accessing the site via cache could be served altered or malicious content without the Figma server detecting it.

HTTP Response Overview:

The following HTTP response was analyzed, which indicates potential areas of concern for web cache poisoning:

HTTP/1.1 200 OK
Date: Sat, 19 Oct 2024 23:13:41 GMT
Content-Type: text/html; charset=utf-8
Connection: close
x-sorting-hat-podid: 370
x-sorting-hat-shopid: 57683640503
x-storefront-renderer-rendered: 1
set-cookie: keep_alive=865f7155-7cba-4d00-9740-d40141454c12; path=/; expires=Sat, 19 Oct 2024 23:43:40 GMT; HttpOnly; SameSite=Lax
set-cookie: secure_customer_sig=; path=/; expires=Sun, 19 Oct 2025 23:13:40 GMT; secure; HttpOnly; SameSite=Lax
set-cookie: localization=IN; path=/; expires=Sun, 19 Oct 2025 23:13:40 GMT

set-cookie: cart_currency=INR; path=/; expires=Sat, 02 Nov 2024 23:13:40 GMT
...
x-cache: hit, server
x-frame-options: DENY
content-security-policy: block-all-mixed-content; frame-ancestors 'none';
upgrade-insecure-requests;
strict-transport-security: max-age=7889238
x-shopid: 57683640503
x-shardid: 370
vary: Accept
content-language: en-IN

Key Findings:

1. Cache-Control and Headers:

No explicit cache-control header indicating private or no-cache.

The response contains x-cache: hit, server, showing that responses are being cached.

The presence of cookies (secure_customer_sig, cart_currency) in the response may affect how cache servers treat the request, potentially leading to user-specific data being cached for broader access.

2. Lack of Cache Segmentation:

The vary header includes Accept, but additional headers, such as User-Agent or Cookie, should be included to prevent cache mixing based on different user configurations.

Impact:

Exploitation Potential:

Attackers can exploit this vulnerability by sending specially crafted requests that manipulate cache content, tricking the cache server into storing and serving harmful content to subsequent visitors.

Affected Users:

Any user visiting the Figma store could receive poisoned content due to shared caches across sessions, browsers, or regions.

Timeline:

Issue Discovered: October 19, 2024

Reported By: Srija Paul

This vulnerability, if exploited, could lead to significant data breaches and user security issues on Figma's platform. Prompt mitigation is advised.