Gmail Nawab Khan <nawabkh2040@gmail.com>

Bug Report: JWT Bug in Bill Desk Payment Gateway

1 message

Nawab Khan <nawabkh2040@gmail.com> Tue, Oct 31, 2023 at 5:38 PM
To: support@billdesk.com
Cc: hod.cs@sdbc.ac.in

Dear Bill Desk Payment Gateway Support Team,

I hope this message finds you well. I am writing to report a critical bug in the Bill Desk Payment Gateway, specifically related to the JWT (JSON Web Token) handling. This bug has the potential to convert failed payment responses into successful ones, which I believe is a serious security and financial concern that needs immediate attention.

Bug Details:

Bug Type: JWT Manipulation
Severity: Critical
Description: The Bill Desk Payment Gateway appears to have a vulnerability that allows attackers to manipulate the JWT tokens generated during payment transactions. By exploiting this vulnerability, attackers can change the status of a failed payment response to appear as a successful payment, which poses a significant security and financial risk.
Proof of Concept (PoC):

To demonstrate the issue, I have prepared a Proof of Concept (PoC) that showcases how the JWT manipulation can occur. You can access the PoC through the following link: https://drive.google.com/file/d/17fPUSKXrAX2rqZ_yG3hNLvVfGQ0UY3N0/view?usp=sharing

we have demonstrate with college permission

I kindly request your team to review the PoC and investigate the issue promptly. This vulnerability could potentially lead to fraudulent transactions, financial losses, and a compromised payment gateway reputation.

Steps to Reproduce:

To replicate the issue:

Perform a payment transaction that results in a failed response.
Intercept the JWT token generated during the failed transaction.
Modify the token to indicate a successful payment.
Resubmit the token, which may now result in a successful payment response.
Please take immediate action to address this issue and ensure the security and integrity of the Bill Desk Payment Gateway. I recommend conducting a thorough security audit and implementing necessary fixes to prevent such manipulation of JWT tokens.

I understand the importance of resolving such critical issues promptly and am available to provide any additional information or assistance that your team may require to address this bug effectively.

Additionally, I kindly request that you consider offering a bounty or reward for identifying and responsibly disclosing this security vulnerability. A reward program can encourage security researchers to proactively report issues, ultimately strengthening the security of your payment gateway.

Kindly acknowledge the receipt of this report and keep me updated on the progress of the investigation and any subsequent actions taken to rectify the issue. If you require further details or assistance, please do not hesitate to reach out to me at [Your Email Address].

Thank you for your prompt attention to this matter. I look forward to the resolution of this critical security concern.

Sincerely,

Nawab Khan
+91 8962507486
nawabkh2040@gmail.com