Vulnerability Report - Stored XSS Leading to Account Takeover in Movidesk System (Integrated with Zenvia)

1. Summary:
A critical **Stored Cross-Site Scripting (XSS)** vulnerability has been identified in the Movidesk system when integrated with Zenvia's email services. This vulnerability enables an attacker to perform an **Account Takeover (ATO)** by stealing session cookies due to the lack of the HttpOnly flag on authentication cookies.

2. Vulnerability Details:

- **Vulnerability Type:** Stored XSS (Cross-Site Scripting)
- **Severity:** Critical (CVSS Score suggested: 9.0)
- **Impact:** Account Takeover via Session Hijacking
- **Affected System:** Movidesk (when used with Zenvia email integration)

3. Description:
The vulnerability is triggered through the email integration feature between Zenvia and Movidesk. When an attacker sends an email to a known service address of the target company, the **subject line** of the email is automatically processed and displayed in a new support ticket within Movidesk. The system fails to properly sanitize or escape special characters in the email subject, allowing malicious scripts to be stored and executed when viewed by an authenticated agent.

This attack vector is particularly dangerous because:

- It **bypasses traditional network firewalls and WAFs**, as the malicious payload is delivered through legitimate email traffic.
- The exploit requires minimal interaction; the victim only needs to open the support ticket, which happens as part of their normal workflow.

4. Exploitation Steps:

1. Identify the **service email address** used by the target company's Movidesk system.
2. Craft a malicious email with an XSS payload in the **subject line**, e.g.:
3. "><img src="https://YOUR-WEBHOOK/">
4. Send the email to the target.
5. When the Movidesk system automatically creates a ticket, the subject (with the malicious payload) is stored and later rendered without proper sanitization.

6. As soon as a support agent opens the ticket, the malicious script executes in their browser, stealing session cookies.
7. Since the HttpOnly flag is **not set** on the cookies, the attacker can capture the session and perform an **account takeover**.

5. Impact:

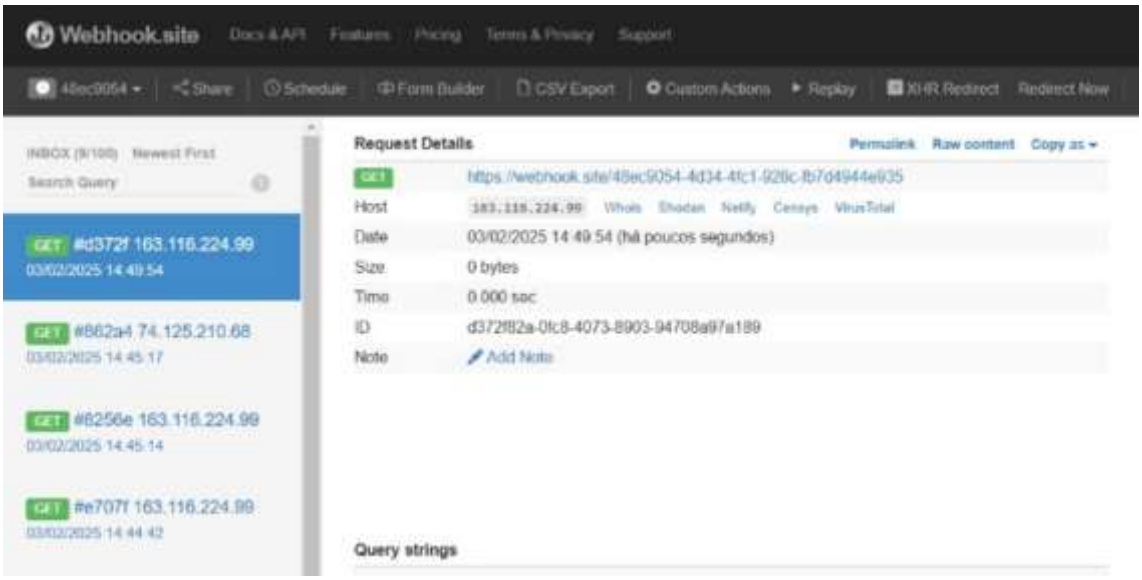
- **Account Takeover:** Full control of the victim's account, including access to sensitive internal data.
- **Data Exposure:** Possibility of lateral movement to other accounts if session cookies are reused across different systems.
- **Network Security Risk:** The attack can bypass traditional security controls, as it originates from legitimate internal workflows.

6. Mitigation Recommendations:

1. **Input Sanitization:** Apply strict sanitization and encoding to all user inputs, especially for data rendered from external sources like emails.
2. **Secure Cookie Attributes:** Set the HttpOnly and Secure flags on all session cookies to prevent client-side access.
3. **Content Security Policy (CSP):** Implement a strong CSP to mitigate XSS impact.
4. **Email Filtering:** Apply server-side filters to detect and block potentially malicious email subjects.

7. Proof of Concept (PoC):

- Payload: "><img src="https://webhook.site/48ec9054-4d34-4fc1-928c-fb7d4944e935">



8. Additional Notes:

- This vulnerability affects all versions of Movidesk integrated with Zenvia that process emails without proper sanitization.
- Testing was conducted in a controlled environment without impacting real users or data.

Reporter: Yago Martins

This report is confidential and intended solely for the vendor's security team until the vulnerability is resolved.