Systems and Network Programming - IE2012

Assignment

Ashan G Punchihewa

IT22327680

Table of Contents

1 Abstract

In the changing field of cybersecurity it has become increasingly important to identify and fix vulnerabilities, in software and systems with the integration of artificial intelligence (AI). This report focuses on CVE-2023-3971 a record in the Common Vulnerabilities and Exposures (CVE) database that addresses a HTML injection vulnerability found in Red Hat Ansible Automation Platform. The analysis covers aspects including website affected by AI integration techniques used for exploitation assessment of impact and strategies for mitigation. Considering its score of 5.4 (MEDIUM) this HTML injection vulnerability is evaluated for its effects on system integrity caused by AI driven factors. The report concludes by emphasizing the need for efforts within the field of cybersecurity and provides references for exploration. Urgent attention and remediation are emphasized to maintain trust and security, in systems infused with AI.

2 CVE-2023-3971

2.1 Introduction

The Common Vulnerabilities and Exposures (CVE) system plays a role, in the field of cybersecurity as it provides an approach for identifying and tracking vulnerabilities. In this report we will explore CVE-2023-3971, which's an HTML injection flaw discovered in the Controller component of the Red Hat Ansible Automation Platform. We will delve into the specifics of this vulnerability its impact. Recommended mitigation strategies.

2.2 CVE Details

2.2.1 CVE Identifier

CVE-2023-3971

2.2.2 Type of Vulnerability

HTML Injection

2.2.3 Description

The vulnerability we are discussing is related to an HTML injection flaw found in the Controller component of the Red Hat Ansible Automation Platform. This flaw enables attackers to inject HTML code allowing them to create a customized login page that can capture credentials potentially leading to a compromise.

2.3 Vulnerable webpage

Red Hat Ansible Automation Platform (version unknown)

2.4 Exploitation

2.4.1 Exploitation Details

This vulnerability arises from a function within the Controller/Hub component resulting in site scripting (XSS). Due to handling of input data attackers are able to inject HTML code posing a risk as they can obtain credentials and compromise the affected systems integrity.

2.4.2 Attack Vectors

To exploit this vulnerability remote initiation is required along with some form of user interaction. This aligns with ATT&CKs T1059.007 technique that denotes a method, for launching such attacks.

2.5 Impact

2.5.1 Potential Impact

If the vulnerability CVE-2023-3971 is successfully exploited it could lead to consequences. These include gaining access, to information compromising user credentials and causing a complete loss of system integrity.

2.5.2 Risks and Threats

There are several risks associated with this vulnerability, such as unauthorized access to sensitive data compromising user credentials and potentially causing a loss of system integrity.

2.6 Mitigation

2.6.1 Vendor Response

The vulnerability was reported on 07/27/2023. As per the information there is currently no publicly known exploit, for this issue. Red Hat, Inc. Has acknowledged the problem as mentioned in the provided references.

2.6.2 Mitigation Strategies

Considering the details provided it is advisable to implement the following strategies, for mitigation,

1. Keep the Red Hat Ansible Automation Platform regularly updated to its version.
2. Incorporate input validation and sanitation measures to counteract any characters in user input thereby preventing HTML injection attacks.

2.7 Conclusion

2.7.1 Summary

The presence of CVE-2023-3971 highlights a vulnerability related to HTML injection in the Red Hat Ansible Automation Platform. This emphasizes the importance of addressing issues. The potential consequences include access to data, compromise of user credentials and potential system integrity loss. Although there is currently no known exploit mitigating these risks involves software updates and adherence to secure coding practices.

The realm of cybersecurity is ever evolving, with new vulnerabilities emerging. The case of CVE-2023-3971 underscores the role played by security professionals, vendors and end users in preserving software system integrity. Staying vigilant, responding promptly to vulnerabilities and fostering collaboration are aspects of maintaining a cybersecurity posture.

2.8 References

2.8.1 External References

- Red Hat CVE-2023-3971 - https://access.redhat.com/security/cve/CVE-2023-3971.

2.8.2 Vendor Advisories

- RHSA-2023:4340 - https://access.redhat.com/errata/RHSA-2023:4340.
- RHSA-2023:4590 - https://access.redhat.com/errata/RHSA-2023:4590.