VASCO Security Advisory

Reflected cross-site scripting vulnerability in IDENTIKEY Authentication Server help function

Advisory ID: vasco-sa-20151126-ias

Revision number: 1.0

Date and time of release: November 26 2015 12:00 UTC

Date and time of last update: November 26 2015 12:00 UTC

Summary

Certain versions of Apache Struts are affected by a cross-site scripting vulnerability when debug mode is switched on or when JSPs are exposed in a production environment. These versions of Apache Struts are being used in IDENTIKEY Authentication Server. Even though the debug mode is switched off, some JSPs are directly accessible on the IAS server.

Impacted products

- IDENTIKEY (Virtual) Appliance versions 3.8 and earlier
- IDENTIKEY Authentication Server versions 3.8 and earlier

Detailed description of vulnerability

The Apache Struts project announced in October 2015 that Apache Struts version 2.0.0 up to version 2.3.16.3 are affected by a cross-site scripting vulnerability when debug mode is switched on or when JSP files are exposed in a production environment. Two CVE identifiers have been assigned to these vulnerabilities:

- CVE-2015-5169: Apache Struts is vulnerable to a cross-site scripting vulnerability when debug mode is enabled. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's web browser within the security context of the hosting Web site, once the URL is clicked.
- CVE-2015-2992: Apache Struts is vulnerable to a cross-site scripting vulnerability when accessing JSP files directly. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked.

Vulnerability CVE-2015-5169 is not applicable to the IDENTIKEY Authentication Service since debug mode is disabled by default.

Vulnerability CVE-2015-2992 is applicable since there are some JSP files that are directly accessible using a browser.

Severity score

The table below denotes the CVSS 2.0 vulnerability score of vulnerability CVE-2015-2992.

CVSS Base Score: 4.3					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Medium	None	None	Partial	None

Product fixes and workarounds

VASCO will fix these vulnerabilities in the following upcoming releases:

- IDENTIKEY (Virtual) Appliance 3.9
- IDENTIKEY Authentication Server 3.9

Customers can protect their IAS-installation by making a modification to the web.xml configuration file. This modification will prohibit direct access to JSP's that should not be directly accessible.

In order to change the configuration, the following security-constraint and security-role must be appended to the web-app body in the web.xml configuration file:

```
<web-app>
   <!-- Restricts access to JSP files - access available only via Struts action -->
   <security-constraint>
      <display-name>No direct JSP access</display-name>
      <web-resource-collection>
         <web-resource-name>No-JSP</web-resource-name>
         <url-pattern>/decorators/*</url-pattern>
         <url-pattern>/include/*</url-pattern>
         <url-pattern>/pages/*</url-pattern>
         <url-pattern>/wizards/*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
         <role-name>no-users</role-name>
      </auth-constraint>
   </security-constraint>

   <security-role>
      <description>Don't assign users to this role</description>
      <role-name>no-users</role-name>
   </security-role>
</web-app>
```

Obtaining product releases with fixes

Customers with a maintenance contract can obtain fixed product releases from MyMaintenance. Customers without a maintenance contract should contact their local sales representative.

References

- Apache Struts security bulletin S2-025 - https://struts.apache.org/docs/s2-025.html
- http://jvn.jp/en/jp/JVN88408929/index.html
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2992

Legal disclaimer