SafeNet Authentication Service Agent for IBM Security Access Manager

Technical Note

gemalto
security to be free

Contents

Introduction

In computer security, a vulnerability is a shortcoming which permits an attacker to lessen a system's data assurance. Cybersecurity vulnerabilities are everywhere, and it is important to take preventive measures to avoid these attacks. The following lists the type of vulnerabilities you may encounter while using the SafeNet Authentication Service (SAS) Agent for IBM Security Access Manager (ISAM), and the recommendations to counter them.

It is always recommended to use HyperText Transfer Protocol Secure (HTTPS) mode for the SafeNet Authentication Service (SAS) Agent for IBM Security Access Manager (ISAM).
There are several types of security certificates that can be used, either your own proprietary certificate or a newly configured one. One recommended method involves using keystore cert for enabling SSL on Tomcat (Click here for details).

Bit Length Vulnerability

The bit length determines the security level of an SSL certificate. The higher the bit length of a key pair (of a certificate), the higher the security level, it provides. For example, a 2048-bit key is stronger, and therefore much harder for a hacker to break into, than a 1024-bit key security.

Recommendations

To ensure higher security, we recommend that you use a digital certificate with a key size of 2048 bits, instead of a 1024-bit key.

HTTP Strict Transport Security Vulnerability

It is important to handle the HTTP Strict Transport Security (HSTS) vulnerability since the absence of a Strict-Transport-Security header (in the response) can cause eavesdropping, man-in-the-middle and active network attacks.

Recommendations

Prerequisite: The Tomcat server should be running in secure mode, and enabled to accept incoming requests for Transport Layer Security (TLS) / Secure Sockets Layer (SSL) connections. The following configuration settings in the server.xml file can help achieve the same:

<Connector port="8080" protocol="HTTP/1.1" <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" secure="true" connectionTimeout="20000" redirectPort="8443" />

<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" secure="true" redirectPort="8443" />

To handle the HSTS vulnerability, add the HSTS feature to the Tomcat server by following the steps:

Uncomment httpHeaderSecurity filter definition in tomcat/conf/web.xml

1. Enable a filter and add a useful max age param

```
<filter>
    <filter-name>httpHeaderSecurity</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
    <init-param>
        <param-name>hstsMaxAgeSeconds</param-name>
        <param-value>899500000</param-value>
    </init-param>
    <async-supported>true</async-supported>
  </filter>
 <filter-mapping>
    <filter-name>httpHeaderSecurity</filter-name>
    <url-pattern>/*</url-pattern>
    <dispatcher>REQUEST</dispatcher>
  </filter-mapping>
```

2. Uncomment filter mapping

```
<filter-mapping>
<filter-name>httpHeaderSecurity</filter-name>
<url-pattern>/*</url-pattern>
<dispatcher>REQUEST</dispatcher>
</filter-mapping>
```

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult the support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can login to manage incidents, get latest software upgrades, and access the Gemalto Knowledge Base.	