CA SiteMinder®

Advanced Password Services Release Notes

12.52 SP1

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Welcome

This document contains information about CA SiteMinder® Advanced Password Services (APS). These notes describe features, operating system support, known issues and fixes.

Chapter 2: New and Changed for Advanced Password Services

Upgrade of CAPKI

CA SiteMinder® is upgraded to use CAPKI 4.3.4 to fix the following OpenSSL vulnerabilities:

- CVE-2014-0224: An SSL/TLS MITM vulnerability exists in OpenSSL 0.9.8y and earlier. An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server.
- CVE-2014-0221: DTLS recursion flaw exists in OpenSSL 0.9.8y and earlier. By sending an invalid DTLS handshake to an OpenSSL DTLS client, the code can be made to recurse, eventually crashing in a DoS attack.
- CVE-2014-3470: Anonymous ECDH denial of service flaw exists in OpenSSL 0.9.8y and earlier. OpenSSL TLS clients enabling anonymous ECDH ciphersuites are subject to a denial of service attack.
- CVE-2014-0076: Fix for the attack described in the paper "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack".

For more information about the vulnerabilities, see the OpenSSL documentation.

Chapter 3: Advanced Password Services Installation and Upgrade Considerations

This section contains the following topics:

Configuration Changes Required for Oracle iPlanet Web Server

To configure APS to work with an Oracle iPlanet web server, add entries to the magnus.conf file of the appropriate web server instance.

Follow these steps:

1. Open *iPlanet_install_dir*/*server_instance*/config/magnus.conf in a text editor.
2. Add the following lines:

   ```
   Init fn="init-cgi" SMPORTAL="webagent_install_dir/bin/SmPortal.cfg"

   APS_LANG_PATH="webagent_install_dir/bin/Language"

   LD_LIBRARY_PATH="webagent_install_dir/bin:webagent_install_dir/ETPKI/lib:<web
   agent installed directory>/lib:webagent_install_dir/ETPKI:/lib:"
   ```

3. Save the magnus.conf file and exit the text editor.

The Oracle iPlanet web server instance is configured to work with APS.

Chapter 4: Advanced Password Services Defects Fixed in 12.51

This section contains the following topics:

APS Uses Unsafe Functions on Windows Server 2008

Symptom:

On Windows Server 2008, Advanced Password Services uses functions deemed unsafe by Microsoft Security Development Lifecycle (SDL).

Solution:

This is no longer an issue. The unsafe functions have been replaced.

Chapter 5: Advanced Password Services Defects Fixed in 12.52

This section contains the following topics:

Forgotten Password Service (FPS) Fails When Configured on Apache HTTP Server (112542)

Symptom:

When an Apache HTTP Server is configured to serve the Forgotten Password Service JSP files, Apache returns a 500 Internal Server Error message instead of the JSP page.

Solution:

The default sample JSP pages that are provided with the Forgotten Password Service are not compatible with the latest Apache JSP implementation. Use the new sample JSPs located in the Alternates subdirectory.

Chapter 6: Advanced Password Services Defects Fixed in 12.52 SP1

This release contains no defects fixed.

Invalid APS Error Message (177604)

Symptom:

Customer saw the following message when a user changes their password using APS:

```
[10/15/2013][][17:45:42.011][19783][3664812944][SmAuthUser.cpp:665]
[LogMessage:ERROR:[sm-Server-02740]
[SM-APS-07401] Unable to securebind to LDAP server cAConsumerdirA01:1636 as
uid=c67b131c-1d99-4bd3-b303-a3b597d926d2,ou=xxx,ou=xxx,ou=xxx,dc=xxx,dc=xxx
Error: Invalid credentials
```

Solution:

This message no longer appears.

Star issue 21561240-3

Invalid Weight Error During Password Change (176719)

Symptom:

Error: "[SM-APS-00500]Invalid weight" occurred during password change when the new password is listed in the password dictionary as a restricted word.

Solution:

This problem has been corrected.

Star issues 21545451;1, 21507336;2

smaphistory is Not Updated During the Forgot Password Service (55422)

Symptom:

The password history attribute, smaphistory, is updated only during the Change Password service but not in the Forgot Password service.

Solution:

The issue is no longer valid.

STAR: 21660317-1

Successful Password Change Displays an Error Message (54473)

Symptom:

APS displays an error message instead of an informational message when a user password is changed successfully.

Solution:

This issue is fixed.

STAR: 21561240-03