Technical Advisory

PKWARE

Technical Advisory

Date issued:	5/25/11	**Advisory sent to:**	Customers of the affected products
Effective date:	Immediate	**Products affected:**	SecureZIP Enterprise Edition for z/OS prior to 12.0 SecureZIP Enterprise Edition for i5/OS prior to 10.0.5 SecureZIP Partner using the above products
Technical Support Ticket ID:	None	**Author:**	PSpicer

Summary of Issue: SecureZIP Enterprise Edition for z/OS prior to 12.0 and SecureZIP Enterprise Edition for i5/OS prior to 10.0.5, cannot process SHA-2[1] signed certificates.

Detailed Description of Issue:
Prior to version 12.0 for z/OS and 10.0.5 for i5/OS, SecureZIP used the RSA BSAFE libraries for cryptographic services. These libraries do not provide support for certificates signed using SHA-2 and will fail while attempting to process such a certificate. This will in turn cause a failure of SecureZIP.

Most commercial certificate authorities are not yet issuing SHA-2 signed certificates, but beginning with RACF for z/OS 1.12, certificates generated with key lengths greater than or equal to 2048 will always use SHA-256 (a SHA-2 algorithm). A 1024-bit key size will continue to use SHA-1.

Customers could unknowingly attempt to process SHA-2 signed certificates using older versions of SecureZIP for z/OS and i5/OS and experience a product failure.

Diagnosing the Issue: Evidence of encountering a certificate having internal SHA-2 hashing may be seen with a combination of the following unexpected messages

For z/OS:

ZPCM024C	CERT_OPEN_FAILURE UNUSABLE
ZPEN037C	Unknown/Missing from Store

For i5/OS:

AQZ0170	Cert Open Failure
AQZ0423	Archive was Signed by "Unknown/Missing from Store" but NOT verified

In both cases additional messages may be displayed and there will be variation depending on the certificate encountered and its intended use.

An external certificate management tool should be used to display the attributes of the certificate to determine its internal hashing algorithm.

Solution: Upgrade to SecureZIP for z/OS 12.0.2 or SecureZIP for i5/OS 10.0.5. This free upgrade for customers with active maintenance uses the OpenSSL cryptographic library which provides support for SHA-2 signed certificates. SecureZIP Partner customers should download the latest version of SecureZIP Partner for z/OS or i5/OS from the Partner Portal.

Proprietary Information: No

* If you need any further information, please contact Product Management

[1] **SHA-2** is a set of cryptographic hash functions (**SHA-224, SHA-256, SHA-384, SHA-512**) designed by the National Security Agency (NSA).