



SHA1 Deprecation

Software version: 9.10, 9.11, and 9.2

Document release date: January 2016

Software release date: January 2016

Contents

- Issue that Requires Attention..... 2**
- Impact on BSAE 2**
- Immediate Mitigation..... 2**
- Send documentation feedback 7**
- Legal notices 7**
 - Warranty..... 7
 - Restricted rights legend..... 7
 - Copyright notice 7
 - Trademark notices..... 7
 - Documentation updates..... 7
 - Support..... 7

Issue that Requires Attention

SHA1 Deprecation

<https://community.qualys.com/blogs/securitylabs/2014/09/09/sha1-deprecation-what-you-need-to-know>


Certificates used by secure websites are signed using hashing algorithms. SHA1 is one such hashing algorithm. Feasibility of breaking SHA1 has increased in the recent past and can lead to potential exposure of secure communication. Microsoft, Google and Mozilla have recently announced they won't be accepting SHA1 certificates post 2016.

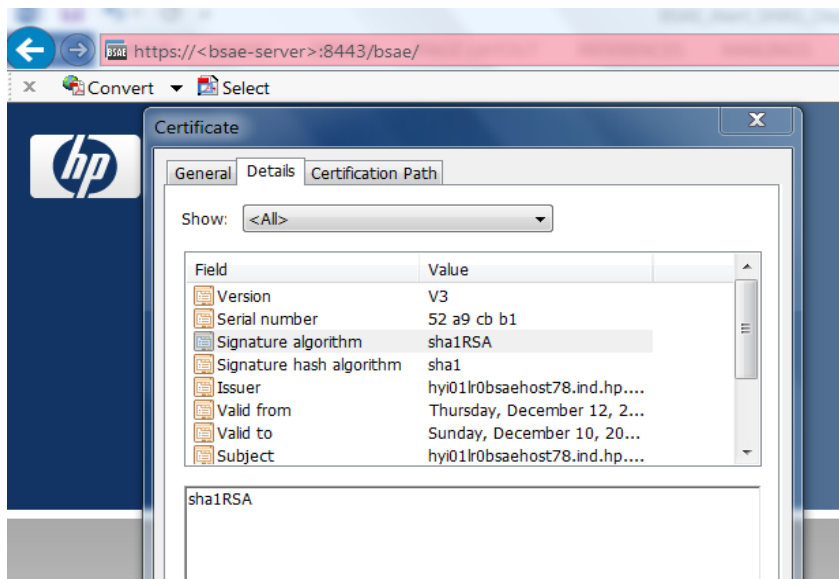
Impact on BSAE

BSAE creates self-signed certificates using SHA1 algorithm during installation. They are used for secure communication between BSAE core and various clients (browsers, java desktop client, dataminer).

All supported releases of BSAE are found to be Vulnerable.

You can check the signature algorithm of BSAE certificate using following steps:

1. Connect to BSAE server using Internet Explorer.
URL - <https://<BSAE-Server>:8443>
2. Click the **Lock** icon , which is located to the right of the Address bar
3. Click "View Certificates" which will display general information of the certificate.
4. Go to "Details" tab. See "Signature Algorithm" field with value as "sha1RSA".



Immediate Mitigation

Remove certificates signed using SHA1 and generate certificates signed using SHA256 algorithm.

The following changes need to be performed on the BSAE core, irrespective of the installation type (i.e., Single or Dual server). No changes are needed on the database server in the case of a Dual server. Please note that HP Support can assist you with the following steps.

1. Stop all running BSAE Essentials data miners. Log in to each system where a data miner is installed and do the following:
 - a. Change to the directory where the data miner is installed. For example:


```
# cd /opt/opsware/dataminer
```
 - b. Stop the data miner by executing the following command:


```
# ./dataminer.sh stop
```
2. Have all data miners complete any pending file transfers. On each system where a data miner is installed, execute the following commands:
 - a. Change to the directory to where the data miner is installed. For example:


```
# cd /opt/opsware/dataminer
```
 - b. Complete any pending file transfers as follows:


```
# ./dataminer.sh start --flushdatafiles ; tail -f dataminer.log
```

When all pending files are successfully transferred, the log file will record "All existing files transferred to server. Exiting..." and the data miner will automatically exit.

3. Login to BSAE Core system as root.
4. Wait for the any pending data to load by checking the `/var/log/opsware/omdb/server.log` file to see if any data is being processed. Make sure no failure has occurred by executing a "find `/var/opt/opsware/omdb/collect`". Unless the flag is set to keep data files, there should be zero files found.
5. Stop the BSAE service on the core machine using one of the following commands, depending on your BSAE version:

For 9.2:

```
# /etc/init.d/bsae stop
```

For 9.1x

```
# /etc/init.d/opsware-omdb stop
```

```
# /etc/init.d/bsae-bo stop
```

6. Backup current keystores and dmboot.pem file on the server by executing the following commands:


```
# cd /var/opt/opsware/crypto/omdb
# cp server.keystore server.keystore_save
# cp server.keystore.bsae-tomcat-create-keystore server.keystore.bsae-tomcat-create-keystore_save
# cd /opt/opsware/omdb/dist
# cp dmboot.pem dmboot.pem_save
```
7. Re-generate keystores and dmboot.pem.
 - a. Change to BSAE crypto directory:


```
# cd /var/opt/opsware/crypto/omdb
```
 - b. Create server.keystore. Replace `<crypto_password>` parameter with your crypto password.


```
# /opt/opsware/jdk1.6/bin/keytool -selfcert -keystore server.keystore -alias omdb -storepass <crypto_password> -keypass <crypto_password> -keyalg RSA -sigalg SHA256withRSA -validity 3650 -dname "cn=`hostname`,ou=server,dc=opsware,dc=com" -storetype JKS -provider com.sun.crypto.provider.SunJCE -noprompt
# /opt/opsware/jdk1.6/bin/keytool -selfcert -keystore server.keystore -alias tomcatbo -storepass <crypto_password> -keypass <crypto_password> -keyalg RSA -sigalg SHA256withRSA -validity 3650 -dname "cn=`hostname`,ou=server,dc=opsware,dc=com" -storetype JKS -provider com.sun.crypto.provider.SunJCE -noprompt
```
 - c. Create server.keystore.bsae-tomcat-create-keystore. Replace `<crypto_password>` parameter with your crypto password.


```
# /opt/opsware/jdk1.6/bin/keytool -selfcert -keystore server.keystore.bsae-tomcat-create-keystore -alias tomcatbo -storepass <crypto_password> -keypass <crypto_password> -keyalg RSA -sigalg SHA256withRSA -validity 3650 -dname "cn=`hostname`,ou=server,dc=opsware,dc=com" -storetype JKS -provider com.sun.crypto.provider.SunJCE -noprompt
```
 - d. Regenerate dmboot.pem file by executing the following commands. Replace `<crypto_password>` parameter with your crypto password.


```
# cd /opt/opsware/omdb/dist
```

```
# /opt/opsware/jdk1.6/bin/keytool -export -rfc -alias omdb -keystore /var/opt/opsware/crypto/omdb/server.keystore -storepass <crypto_password> -file dmboot.pem
```

8. On the BSA Essentials server, reset all of the registered data miners by executing the following commands:

a. Change directory as follows:

```
# cd /opt/opsware/omdb/bin
```

b. List the registered data miners to determine their names as follows:

```
# ./dmconfig.sh -list
```

c. Reset each registered data miner as follows:

```
# ./dmconfig.sh -reset -name <registered Data Miner name>
```

9. Start BSA Essentials services on the server by executing the following commands:

For 9.2:

```
# /etc/init.d/bsae start
```

For 9.1x

```
# /etc/init.d/bsae-bo start
```

```
# /etc/init.d/opsware-omdb start
```

10. Log into each system where a data miner is installed and execute the following commands:

a. Change to the directory where the data miner is installed. For example:

```
# cd /opt/opsware/dataminer
```

b. Save the current data miner keystore as follows:

```
# mv dataminer.keystore dataminer.keystore_save
```

c. Replace dmboot.pem file with the one that was generated on the BSA Essentials server after saving the current one by executing the following commands:

```
# mv dmboot.pem dmboot.pem_save
```

```
# scp root@<BSAE server>:/opt/opsware/omdb/dist/dmboot.pem dmboot.pem
```

```
# chown root:root dmboot.pem
```

d. Start the data miner by executing the following command:

```
# ./dataminer.sh start
```

The data miner should successfully connect and you should see that it has registered with the BSA Essentials server.

e. You can verify the data miner successfully registered by executing the following commands on the BSA Essentials server:

```
# cd /opt/opsware/omdb/bin
```

```
# ./dmconfig.sh -list
```

The active flag (set to 0 by the reset done previously) should now be set to 1.

11. Update dataminer.tar distributions with new dmboot.pem file. Log in to BSAE Essentials server:

a. Change to dataminer distributions directory:

```
# cd /opt/opsware/omdb/dist/
```

b. Backup dataminer distributions:

```
# cp dataminer.tar dataminer.tar_save
```

```
# cp dataminer-upgrade.tar dataminer-upgrade.tar_save
```

```
# cp dataminer.zip dataminer.zip_save
```

```
# cp dataminer-upgrade.zip dataminer-upgrade.zip_save
```

c. Update dataminer distributions:

```
# tar -uvf dataminer.tar dmboot.pem
```

```
# tar -uvf dataminer-upgrade.tar dmboot.pem
```

```
# zip dataminer.zip dmboot.pem
# chown omdb:omdb dataminer.zip
# zip dataminer-upgrade.zip dmboot.pem
# chown omdb:omdb dataminer-upgrade.zip
```

12. Verify newly created BSAE certificates are signed using SHA256 algorithm. See steps listed in Page 2 “Impact on BSAE” section to view the signature algorithm of regenerated certificates. “Signature algorithm” field should display the value “sha256RSA”

Steps to Rollback

In case you want to undo the changes and use the old SHA1 certificates, following are the steps:

1. Perform steps 1 to 5 listed above.

2. Rollback keystores and dmboot.pem files

```
# cd /var/opt/opsware/crypto/omdb
# mv server.keystore_save server.keystore
# chown omdb:omdb server.keystore
# chmod 700 server.keystore
# mv server.keystore.bsae-tomcat-create-keystore_save server.keystore.bsae-tomcat-create-keystore
# chmod 664 server.keystore.bsae-tomcat-create-keystore
# cd /opt/opsware/omdb/dist
# mv dmboot.pem_save dmboot.pem
# chown omdb:omdb dmboot.pem
# chmod 664 dmboot.pem
```

3. On the BSA Essentials server, reset all of the registered data miners by executing the following commands:

- a. Change directory as follows:

```
# cd /opt/opsware/omdb/bin
```

- b. List the registered data miners to determine their names as follows:

```
# ./dmconfig.sh -list
```

- c. Reset each registered data miner as follows:

```
# ./dmconfig.sh -reset -name <registered Data Miner name>
```

4. Start BSA Essentials services on the server by executing the following commands:

For 9.2:

```
# /etc/init.d/bsae start
```

For 9.1x

```
# /etc/init.d/bsae-bo start
```

```
# /etc/init.d/opsware-omdb start
```

5. Log into each system where a data miner is installed and execute the following commands:

- a. Rollback dataminer.keystore and dmboot.pem

```
# cd /opt/opsware/dataminer
```

```
# rm -f dataminer.keystore
```

```
# mv dmboot.pem_save dmboot.pem
```

- b. Start the data miner by executing the following command:

```
# ./dataminer.sh start
```

The data miner should successfully connect and you should see that it has registered with the BSA Essentials server.

c. You can verify the data miner successfully registered by executing the following commands on the BSA Essentials server:

```
# cd /opt/opsware/omdb/bin
```

```
# ./dmconfig.sh -list
```

The active flag (set to 0 by the reset done previously) should now be set to 1.

6. Rollback dataminer.tar distributions. Log in to BSAE Essentials server:

```
# cd /opt/opsware/omdb/dist/
```

```
# mv dataminer.tar_save dataminer.tar
```

```
# chown omdb:omdb dataminer.tar
```

```
# mv dataminer-upgrade.tar_save dataminer-upgrade.tar
```

```
# chown omdb:omdb dataminer-upgrade.tar
```

```
# mv dataminer.zip_save dataminer.zip
```

```
# chown omdb:omdb dataminer.zip
```

```
# mv dataminer-upgrade.zip_save dataminer-upgrade.zip
```

```
# chown omdb:omdb dataminer-upgrade.zip
```

Send documentation feedback

If you have comments about this document, you can send them to hpe_sa_docs@hpe.com.

Legal notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notice

© Copyright 2015 Hewlett Packard Enterprise Development LP

Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register: <https://softwaresupport.hp.com/>

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard Enterprise sales representative for details.

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at <https://softwaresupport.hp.com/>