K76313281: The BIG-IP system may advertise unsupported SHA algorithms erroneously when performing certificate authentication with the TLSv1.2 protocol

Known Issue

Original Publication Date: Oct 31, 2016

Update Date: Mar 14, 2017

Known Issue

The BIG-IP system may advertise unsupported SHA algorithms erroneously when performing certificate authentication with the TLSv1.2 protocol.

This issue occurs when all of the following conditions are met:

- You have a virtual server configured with a Client SSL profile on the BIG-IP system.
- The Client SSL profile has the client certification authentication set to **Request** or **Required**.
- The client attempts to select one of the following unsupported signature algorithms advertised by the BIG-IP system during the Secure Sockets Layer (SSL) handshake process:

    - SHA256-RSA
    - SHA384-RSA
    - SHA512-RSA

Impact

The BIG-IP system may erroneously allow the client to select an unsupported signature algorithm when performing certificate authentication. As a result, the client fails to connect to the virtual server.

Symptoms

As a result of this issue, you may encounter one or more of the following symptoms:

- BIG-IP iHealth lists Heuristic H617888 on the **Diagnostics** > **Identified** > **Medium** screen.
- When SSL debugging is turned on, an error message similar to the following example appears in the **/var/log/ltm** log file:

    debug tmm3[1234]: 01260009:7: Connection error: ssl_hs_rxhello:4489: unsupported version (70)

- The network packet capture shows the failed client connection uses the following signature algorithms during the SSL handshake process:

    - SHA256-RSA (0x0401)
    - SHA384-RSA (0x0501)
    - SHA512-RSA (0x0601)

- The network packet capture shows the successful client connection uses the SHA1-RSA (0x0201) signature algorithm during the SSL handshake process.

Resolution

Status

F5 Product Development has assigned ID 451003 to this issue. F5 has confirmed that this issue exists in the products listed in the **Applies To** box, located in the upper-right corner of this article. For information about releases or hotfixes that resolve this issue, refer to the following table:

Type of Fix	Fixes Introduced In	Related Articles
Release	11.5.0	K2200: Most recent versions of F5 software
Hotfix	11.4.1 HF9 11.2.1 HF16	K9502: BIG-IP hotfix matrix

Workaround

None

Supplemental Information

- K4918: Overview of the F5 critical issue hotfix policy
- K167: Downloading software and firmware from F5
- K17465: Determining if a Known Issue is resolved for a specific BIG-IP version
- K13123: Managing BIG-IP product hotfixes (11.x - 12.x)
- K14819: Troubleshooting client certificate authentication
- K5532: Configuring the level of information logged for TMM-specific events
- K14783: Overview of the Client SSL profile (11.x - 12.x)

Applies to:

Product: BIG-IP, BIG-IP LTM
11.4.1, 11.4.0, 11.3.0, 11.2.1