Secure Web Gateway Version 11.0

Logjam Hotfix [CVE-2015-4000]

This Update provides details of Logjam Hotfix [CVE-2015-4000] for Secure Web Gateway version 11.0.

About this Hotfix

Diffie-Hellman key exchange is a cryptographic algorithm that allows Internet protocols to agree on a shared key and negotiate a secure connection. It is fundamental to many protocols including HTTPS, SSH, and protocols that rely on Transport Layer Security (TLS).

This hotfix addresses weaknesses in how Diffie-Hellman key exchange is deployed, which can result in a Logjam attack against the TLS protocol. The vulnerability is attributable to a flaw in the TLS protocol rather than an implementation vulnerability.

A Logjam attack can affect any server that supports Ephemeral Diffie-Hellman export ciphers, as well as all modern web browsers. The attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography, enabling the attacker to read and modify any data passing over the connection.

Important: This hotfix is part of Trustwave SWG's ongoing response to the Logjam vulnerability in the TLS protocol. Changing circumstances in the field and changes in coding by the various browser developers may require additional action over time.

Known Issues

1. After installing this hotfix, SWG will no longer support cipher suites using authenticated ephemeral Diffie-Helman (EDH) key agreements. Some websites will only negotiate TLS with this cipher, and so will no longer work. If the operation of such websites is critical, you can revert the change and allow SWG to use that cipher again.

   If the system must be reverted back to support EDH, contact Trustwave Support at tac@trustwave.com.
2. Any future Management hotfix applied to the Policy Server will revert this change. **This hotfix cannot be reapplied afterwards**.
3. After any future migration to SWG version 11.5, the string affected by this hotfix will not be recognized and the system will downgrade to a **WEAK cipher list**. For each device, the **Allow Weak Ciphersuites** check box in **Devices > HTTPS > Advanced** tab will be updated automatically and should be unchecked to return to usage of strong ciphers only.

   In addition, Logjam Hotfix CVE-2015-4000 for SWG 11.5 must be applied after the migration to version 11.5.

Installation Details

Important Notes:

- This Hotfix must be installed by the SWG administrator on top of **SWG 11.0**.
- Management Hotfix 08-01 for SWG 11.0 must be applied **before** applying this hotfix.
- This Hotfix restarts the Scanning Server and will therefore impact user Web access for some minutes.

Installation

To install this Hotfix (if you have already downloaded the Hotfix file, ignore steps 1-4):

1. For each device under **Devices**, select **HTTPS** and in the **Advanced** tab, uncheck the **Allow Weak Ciphersuites** check box.
2. Download the Hotfix from the FTP site to your local desktop. Note that you can verify the Hotfix content using the md5 utility against the md5 file from the FTP.
3. In the Management Console, navigate to **Settings > Updates > Updates Management**.
4. Click **Import Updates** at the lower right of the screen.
5. In the Local Update Import window that opens, browse to the Hotfix **fup** file on your desktop; select it and click **Upload** in the window. The Hotfix will appear in the Available Updates window. If it does not appear right away, click the **Refresh** button.
6. In the Available Updates window, select the Hotfix from the list and click **Install Update**. Once the Hotfix has been installed, it will move to the Installed Updates tab.

Legal Notice

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: tac@trustwave.com

Trademarks

About Trustwave®

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations — ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers — manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide.

For more information, visit https://www.trustwave.com.