National Computer Board
Computer Emergency Response Team of Mauritius
(CERT-MU)

Targeted Security Alert

LOGJAM ATTACK

Original Issue Date: May 21, 2015

Severity Rating: High

Affected Systems:

- Browsers

Description:

A new vulnerability has been identified dubbed as Logjam and affects a range of commonly used secure communication services including Transport Layer Security (TLS), Secure Shell (SSH) and IPSec. According to security researchers, the Logjam attack is an offshoot of the FREAK vulnerability discovered in March. This vulnerability exploits a weakness in the critical session key exchange mechanism that takes place at the start of secure communications when sessions are being negotiated between the communicating parties. Successful exploitation of this vulnerability could allow an attacker to carry out an attack by injecting themselves into communications between a client and a server as a man-in-the-middle (MITM). This could be carried out in places offering public Wi-Fi such as an airport or cafe. The attack could also be carried out if the attacker can gain access to a wired network to intercept network traffic. Attackers who already have a network presence could potentially carry out this attack on a corporate network.

Methodology:

The Logjam attack works since it allows an attacker to make a client/server key exchange process use much weaker protection. By manipulating the session key negotiation process, an attacker could force the use of an export-grade Diffie-Hellman key exchange mechanism for transporting session keys. Export-grade encryption uses 512-bit keys which, along with other factors in widely used implementations can allow attackers to break the encryption and discover the session key being exchanged. The downgrade mechanism is similar to the FREAK vulnerability in which an attacker could force client and servers communicating on SSL/TLS to downgrade to export grade encryption which is easier to break.

Impact:

Successful exploitation of this vulnerability can result into loss of secrecy. Many users depend on secure channels to exchange sensitive information such as usernames, passwords, card information when using

online services. This attack could compromise the secure channel, allowing the attacker to read and manipulate information that should be secure.

Workarounds:

1. Users are advised to update their browsers to the latest versions when become available. All major browser vendors are already working on the latest patches to address this vulnerability.

2. Corporate users are advised to disable support for export-grade cipher suites. This will help to address FREAK as well as Logjam. Administrators are also advised to use a unique 2048-bit strength Diffie-Hellman group for key exchange.

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info: contact@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu