National Computer Board

Computer Emergency Response Team of Mauritius

(CERT-MU)

Targeted Security Alert

FREAK SSL/TLS Vulnerability Attack

Original Issue Date: March 09, 2015

Severity Rating: High

System Affected:

Servers

- OpenSSL
- Microsoft Schannel
- Apple SecureTransport

Browsers

- Internet Explorer
- Chrome on Mac OS
- Chrome on Android
- Safari on Mac OS
- Safari iOS
- Stock Android Browser
- Blackberry Browser
- Opera on Mac OS
- Opera on Linux

Description:

The FREAK attack is a new SSL/TLS vulnerability. It allows an attacker to intercept HTTPS connections between vulnerable clients and servers and force them to use weakened encryption, which the attacker can break to steal or manipulate sensitive data. The FREAK attack is possible when a vulnerable browser connects to a susceptible web server—a server that accepts "export-grade" encryption.

Solution:

Server

Immediately disable support for TLS export cipher suites and also disable other cipher suites that are known to be insecure and enable forward secrecy.
To check if your server is vulnerable through an online tool please click here.

Browser (End-Users)

Make sure to have the most recent version of the browser installed, and check for updates frequently. Updates that fix the FREAK attack should be available for all major browsers soon.
To check if your browser is vulnerable through an online tool please click here.

System Administrator and Developer

Make sure any TLS libraries you use are up to date. Unpatched OpenSSL, Microsoft Schannel, and Apple SecureTransport all suffer from the vulnerability. Note that these libraries are used internally by many other programs, such as wget and curl. Also ensure that the software does not offer export cipher suites, even as a last resort, since they can be exploited even if the TLS library is patched.

CVE Information

CVE-2015-1637

References

University of Michigan – FREAK Attack

https://freakattack.com/

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