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

Threat Alert

The HeartBleed Bug

Issued on: April 10, 2014

Severity Rating: High

Systems Affected:

- OpenSSL 1.0.1 through 1.0.1f (inclusive) versions

Operating system distributions with potentially vulnerable OpenSSL version are:

- Debian Wheezy (stable), OpenSSL 1.0.1e-2+deb7u4
- Ubuntu 12.04.4 LTS, OpenSSL 1.0.1-4ubuntu5.11
- CentOS 6.5, OpenSSL 1.0.1e-15
- Fedora 18, OpenSSL 1.0.1e-4
- OpenBSD 5.3 (OpenSSL 1.0.1c 10 May 2012) and 5.4 (OpenSSL 1.0.1c 10 May 2012)
- FreeBSD 10.0 - OpenSSL 1.0.1e 11 Feb 2013
- NetBSD 5.0.2 (OpenSSL 1.0.1e)
- OpenSUSE 12.2 (OpenSSL 1.0.1c)

Description:

A critical vulnerability has been identified in OpenSSL cryptographic software library. OpenSSL is an open-source implementation of the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. This vulnerability known as the "Heartbleed Bug" can allow remote attackers to steal the information protected by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The "Heartbleed Bug" allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys

used to identify the Service Providers and to encrypt the traffic, the names and passwords of the users and the actual content. Successful exploitation of this vulnerability allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

Bug was introduced to OpenSSL in December 2011 and has been out in the wild since OpenSSL release 1.0.1 on 14th of March 2012. OpenSSL 1.0.1g released on 7th of April 2014 fixes the bug.

CVE Information

The CVE provides information about the vulnerability.

CVE-2014-0160

Workarounds

1. Users are advised to change their passwords as a precaution, if they have a Trust Center login
2. Identify if your web servers are vulnerable (running OpenSSL versions 1.0.1 through 1.0.1f with heartbeat extension enabled)
3. Upgrade to the latest patch of OpenSSL 1.0.1g if your server is impacted
4. Reissue any SSL certificates on affected web servers after moving to a patched version of OpenSSL
5. Test your SSL installations
6. Website administrators should also consider resetting end-user passwords as they may have been visible in a compromised server's memory

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : contact@cert-mu.gov.mu

Incident: incident@cert-mu.gov.mu

Website: http://www.cert-mu.org.mu