**Ref: AN110420142**

11th April 2014

All Accounting Officers

Ministries, Departments, Agencies

**Uganda**

**RE: OPEN SSL VULNERABILITIES**

This note is to all administrators of web servers running open SSL.

There is vulnerability, dubbed “Heartbleed”, which is a security concern for users of OpenSSL, a widely-used open source cryptographic software library. It can allow attackers to read the memory of the systems using vulnerable versions of OpenSSL library (1.0.1 through 1.0.1f). This may disclose the secret keys of vulnerable servers, which allows attackers to decrypt and eavesdrop on SSL encrypted communications and impersonate service providers. In addition, other data in memory may be disclosed, which conceivably could include usernames and passwords of users or other data stored in server memory.

If your server is running a version of OpenSSL prior to 1.0.1, no action is required. If your server is running OpenSSL versions 1.0.1 through 1.0.1f with heartbleed extension enabled, then update to the latest patched version of OpenSSL 1.0.1g or recompile OpenSSL **without** the heartbleed extension.

After the update above, generate a new Certificate Signing Request (CSR) and reissue any SSL certificates for affected web servers using the new CSR. Install the new SSL certificate and test your installation. After the new certificate is successfully installed, revoke any certificates that were replaced.

Website administrators should also consider resetting end-user passwords that may have been visible in a compromised server memory.

The National Information Technology Authority of Uganda (NITA-U) shall monitor progress of these activities to confirm compliance. MDAs are therefore required to report back to NITA-U on progress of compliance on a quarterly basis.

For more information please address your concerns to security@cert.ug or security@nita.go.ug.

I look forward to your usual cooperation.

Administrator

**National Computer Emergency Response Team /CC**

**CC: Executive Director, National Information Technology Authority**

**CC: Director Information Security, National Information Technology Authority**