Mutare

Mutare Response to the Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, 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. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.
(source: http://heartbleed.com)

The Heartbleed Bug was brought to the attention of the public Monday April, 7th. Mutare took immediate action. Below are the actions that Mutare has taken.

I. Mutare Audit

a. Audit of all our internal infrastructure, to determine if systems were affected.

II. Mutare Risk Assessment

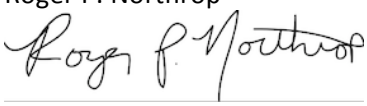
a. Mutare has confirmed that none of our systems are currently at risk due to this vulnerability.

III. Mutare analytics of all data

a. No data has been compromised.
b. No hosted customers were affected.
c. No hosted sites were offline for patching.

If you have any further questions you can contact Mutare in two different ways, call 847-496-9000 and ask for Roger Northrop, or email help@mutare.com with the subject Heartbleed questions, a ticket will be open to have a record of your request.

Sincerely
Roger P. Northrop



CTO, Mutare