Now converted to PDF as email systems will not allow message regardiing this issue to be sent

M

-----Original Message-----
From: Michael Sutton [mailto:michael.sutton@awacs.co.nz]
Sent: Wednesday, 9 April 2014 10:53 a.m.
To: Policy Advisory Group (pag@mailman.internetnz.net.nz)
Subject: Heartbleed - OpenSSL - DNSsec - SSL Certificate revoke and reissue - Embedded systems

For the love of God; this is the fourth attempt to post this message to PAG. I have removed http and changed my smtp mail clients server to a personal smtp server as the network smtp servers seem be intercepting and blocking this email which contains links or content/words within this email which may be considered as a threat.

I have tried to also post to NZNOG but appeared also to be black holed; Dean has posted to NZNOG I think this is a PAG issue as well as it relates to Certificate security DNSsec etc:

xxx://www.kb.cert.org/vuls/id/720951

xxx://heartbleed.com/

This seems to be a "five bells" alarm as it will also include embedded devices world-wide using OpenSSL 1.0.1 - 1.0.1f.

1. In addition to upgrading OpenSSL system wide, should "everyone" be advised to get their existing SSL certificates revoked and reissued as on reading this vulnerability the certs private security keys may/will have been read and compromised ?

2. Should Verisign & Comodo etc be lobbied at the highest government level and locally by the likes of InternetNZ as well as ICANN, APIA to revoke and replace all customers Certs "free of charge" as those existing Certs when used on systems based on OpenSSL have been compromised ?

3. Should those with self-signed certs upgrade their OpenSSL software and regenerate and replace all their existing Certificates ?

4. Does this effect retrospectively the security of DNSsec signed systems ?

5. I note that since last night there has been at least one public site that tests for Heartbleed and that www.govt.nz was vulnerable and has now been patched however if "govt.nz" Certs have been compromised how deep will the problem be.

Comments appreciated.

Michael Sutton
+21 305500

On Behalf Of Dean Pemberton
Sent: Tuesday, 8 April 2014 8:45 p.m.
To: nznog
Subject: [nznog] OpenSSL vulnerability

Here's one to keep an eye on. Seems to be getting a bit of attention.
<snip>
Work with your vendors to confirm if you're at risk.