Replicant - Issue #1029

SSLv3 (aka POODLE) vulnerability - CVE-2014-3566

11/06/2014 09:54 AM - My Self

Status:	Closed	**Start date:**	11/06/2014
Priority:	High	**Due date:**	
Assignee:	Paul Kocialkowski	**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	Any version	**Spent time:**	0.00 hour
Resolution:	fixed	**Grant:**	
Device:		**Type of work:**	

Description

I hope it's a good idea to open a bug ticket about the forum topic: http://redmine.replicant.us/boards/9/topics/6909

Summary
Replicant should be vulnerable to POODLE (= Padding Oracle On Downgraded Legacy Encryption).
CM specific informations:
http://www.theregister.co.uk/2014/10/13/androids_cyanogenmod_open_to_mitm_attacks/
http://www.cyanogenmod.org/blog/in-response-to-the-register-mitm-article

Seems CM 11.0 got a patch:
https://github.com/CyanogenMod/android_external_apache-http/commit/f925f10b1feba92868fd4e8966592ec1bf755d67
respectively:
http://review.cyanogenmod.org/#/c/74106/1/src/org/apache/http/conn/ssl/AbstractVerifier.java
http://review.cyanogenmod.org/#/c/74114/

In CM 10.2 branch, the vulnerable code still seems present:
https://github.com/CyanogenMod/android_external_apache-http/blob/cm-10.2/src/org/apache/http/conn/ssl/AbstractVerifier.java#L228-244

Hope there is an easy way to fix that behavior in Replicant.

History

#1 - 11/08/2014 02:46 PM - Denis 'GNUtoo' Carikli

- Category changed from 51 to Security

That one seems very serious, If I remember well it's a downgrade attack to a weaker encryption, which is "easily" breakable.

Denis.

#2 - 11/10/2014 11:31 AM - My Self

That's correct. More technical informations here: https://www.openssl.org/~bodo/ssl-poodle.pdf
I've verified the vulnerability of Replicant over: https://www.poodletest.com/

#3 - 11/14/2014 02:27 PM - My Self

I've found some more test pages:
https://zmap.io/sslv3/
https://www.ssllabs.com/ssltest/viewMyClient.html
The last one ist the one with the most details...

Furthermore I've found this blog post from the Google Security Team:
http://googleonlinesecurity.blogspot.de/2014/10/this-poodle-bites-exploiting-ssl-30.html

For example reasons, here are the merged commits for this patches from the OMNI project:
https://gerrit.omnirom.org/#/q/topic:%22CVE-2014-3566+%28POODLE%29%22

Hope this helps.

#4 - 11/28/2014 09:22 PM - Paul Kocialkowski

- Status changed from New to Closed

- Resolution set to fixed

Everything pushed to the repositories, will be part of the next batch of images.