How We Discovered Thousands of Vulnerable Android Apps in 1 Day

Joji Montelibano
Vulnerability Analysis Technical Manager
CERT
@certcc

Will Dormann
Vulnerability Analyst
CERT
@wdormann
Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® and CERT Coordination Center® are registered marks of Carnegie Mellon University.

DM-0002136
What is CERT?

- Center of Internet security expertise
- Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today
- Located in the Software Engineering Institute (SEI)
  - Federally Funded Research & Development Center (FFRDC)
  - Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)
CERT Vulnerability Analysis

Mission: Make Software Safer

Vulnerability Coordination

Vulnerability Discovery
Vulnerability Coordination
Is easy?
ActiveX

- Dranzer + HijackThis logs + Automation = Lots of Vulnerabilities
- Vulnerability Detection in ActiveX Controls through Automated Fuzz Testing (Jan 2008) [http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=53466](http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=53466)
ActiveX

- Thousands of vulnerabilities discovered.
- Manual coordination of important/popular ones.
- Many ignored.
ffmpeg

- ffmpeg + BFF = lots of uniquely-crashing testcases

**msg6282 (view)**

**Author:** WD  
**Date:** 2009-06-30 18:28:54

Attached is a zip file with multiple (73) files that cause ffmpeg to crash. The crashers are in a subset of various codecs. Included with each codec/directory are:

1) The seed/good [file](#)
2) Variations of the file that cause crashes (basename.x.y)
3) GDB output for the crashing testcases
4) Valgrind output for the crashing testcases
5) tabriffdump output for the crashing testcases
6) A diff summary of what is different between the crashing testcase and the original file, RIFF-header-wise.

About half of the crashers are something that is in a RIFF header for the file (e.g. ImageHeight, ImageWidth, dsScale, etc.) The other half appear to be something specific decoding of the codec.
On Tue, Jun 30, 2009 at 06:28:54PM +0000, WD wrote:
> Attached is a zip file with multiple (73) files that cause ffmpeg to crash.

A lot of these file crash no longer with SVN, please get rid of those that work now, 73 files are simply too much to handle.
Background

Where am I and how did I get here?
History

- Download.com

http://www.cert.org/blogs/certcc/post.cfm?EntryID=199
The internet is horrible
Identical installers

- Installers from Download.com are the same:
  - 5a275a569dce6e2f2f0284d82d31310b *cbsidlm-cbsi213-Enable__Disable_Registry_Tool-SEO-75812481.exe
  - 5a275a569dce6e2f2f0284d82d31310b *cbsidlm-cbsi213-KMPlayer-SEO-10659939.exe
GET /rest/v1.0/softwareProductLink?productSetId=10659939&partTag=dlm&path=SEO&build=213 HTTP/1.1
Host: api.cnet.com

HTTP/1.1 200 OK

<?xml version="1.0" encoding="utf-8"?>

<CNETResponse xmlns="http://api.cnet.com/restApi/v1.0/ns"
xmlns:xlink="http://www.w3.org/1999/xlink" version="1.0"><SoftwareProductLink id="13819308"
setId="10659939" appVers="1.0"><Name><![CDATA[KMPlayer - 3.9.1.129]]></Name><ProductName><![CDATA[KMPlayer]]></ProductName><ProductVersion><![CDATA[3.9.1.129]]></ProductVersion><FileName><![CDATA[KMPlayer_3.9.1.129.exe]]></FileName><FileSize><![CDATA[35872504]]></FileSize><FileMd5Checksum><![CDATA[5d0e7d17fc4ef0802a9332c83075047c]]></FileMd5Checksum><PublishDate><![CDATA[2014-10-06]]></PublishDate><CategoryId><![CDATA[13632]]></CategoryId><Category><![CDATA[Downloads^Video Software^Video Players]]></Category><License><![CDATA[Free]]></License><DownloadLink>http://software-files-a.cnet.com/s/software/13/81/93/08/KMPlayer_3.9.1.129.exe?token=1413054436_d56f7814cd5af230f782dd28550e85a</DownloadLink><TrackedDownloadLink>http://dw.cbsi.com/redir?edId=1174&amp;siteId=4&amp;lop=feed.dl&amp;ontologyId=13632&amp;tag=tdw_dlm&amp;pid=13819308&amp;destUrl=http://software-files-a.cnet.com/s/software%2F13%2F81%2F93%2F08%2FKMPlayer_3.9.1.129.exe%3Ftoken%3D1413054436_2defb65a1350a3b035964c18f30fb06e%26fileName%3DKMPlayer_3.9.1.29.exe
Just MITM it!

- Set up a proxy to modify content as it’s transferred
- Problem: Installer isn’t proxy-aware!
Solution: CERT Tapioca

- Transparent Proxy Capture Appliance
- UbuFuzz + iptables + mitmproxy
CERT Tapioca

CERT Tapioca is a network-layer man-in-the-middle (MITM) proxy VM that is based on UbuFuzz and is preloaded with mitmproxy. CERT Tapioca is available in OVA format, which should be compatible with a range of virtualization products, including VMware, VirtualBox, and others.

The primary modes of operation are

1) **Checking for apps that fail to validate certificates:**
Simply associate device to access point or connect to network and perform the activity. Any logged https traffic is from software that fails to check for a valid SSL chain.

2) **Investigating traffic of any http/https traffic:**
Install the root CA of the MITM software that you are using into the OS of the device that you are testing.

http://www.cert.org/vulnerability-analysis/tools/cert-tapioca.cfm
How it works

I can see everything if the client doesn’t validate SSL

Invalid SSL handshake

Valid SSL handshake
Tapioca architecture
Tapioca architecture
Investigating Android

- Use a phone and a wireless access point
Improvement #1

◆ Virtualization and Automation
  • google-play-crawler
  • VMware
  • Android SDK
  • AVD
  • Monkeyrunner
  • Monkey

◆ Now I can test when I sleep!

https://github.com/Akdeniz/google-play-crawler
http://www.cert.org/blogs/certcc/post.cfm?EntryID=204
Automated Android
CERT Tapioca
Improvement #2

- Parallelization

- Rather than 1 Android VM and 1 Tapioca VM, what about 20 of each?

- Now I can test 20x faster!
Android emulation annoyance

- ARM Android emulation is slow. Very slow.

- x86 Android emulation is fast (~15x faster), IFF you have a KVM-enabled Linux kernel.
Improvement #3

- Solution: x86 Android in a VM (not an emulator):
  - [http://www.android-x86.org/](http://www.android-x86.org/)
Improvement #4

- Let’s make 20 of them!
Androidx86 SSL Test Architecture

Orchestrator — ADB Net — Androidx86 — MITM Net — CERT Tapioca

Internet
Automation of 20 VMs
Android SSL Coordination

This one’s optimistic
Prior SSL Investigations

- Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security
- October 18, 2012 - Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, Lars Baumgärtner, Bernd Freisleben
- “To evaluate the state of SSL use in Android apps, we downloaded 13,500 popular free apps from Google’s Play Market and studied their properties with respect to the usage of SSL.”
- No app authors contacted?
Prior SSL Investigations

◆ SSL Vulnerabilities: Who listens when Android applications talk?
◆ August 20, 2014 - Adrian Mettler, Vishwanath Raman, Yulong Zhang
◆ “We reviewed the 1,000 most-downloaded free applications in the Google Play store as of July 17, 2014.”
◆ No app authors contacted?
Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information

Mobile Apps Placed Credit Card Details, Credit Report Data, Social Security Numbers at Risk

FOR RELEASE
March 28, 2014

TAGS: deceptive/misleading conduct | Technology | Bureau of Consumer Protection
Notify Affected Authors

Hello,

This is Will Dormann with the CERT Coordination Center, which is part of Carnegie Mellon University. <http://www.cert.org/about>

We've recently been evaluating with CERT Tapioca <http://www.cert.org/blogs/certcc/post.cfm?EntryID=204> the use of SSL by Android apps. Through automated testing, we are logging apps that cause traffic to be sent or received over an HTTPS connection that has an invalid SSL certificate chain.

The following application has demonstrated this incorrect behavior:

APP_ID

Due to the sheer volume of affected applications, we are currently unable to manually inspect every affected application. However, we are sending notifications to the application authors for further investigation.

<SNIP>
Publish the offending apps

https://docs.google.com/spreadsheets/d/1t5GXwjlw82SyunALVJb2w0zi3FoLRLkfGPC7AMjRF0r4/edit?usp=sharing
Listed Applications

- An app is listed in the spreadsheet when it fails dynamic analysis with CERT Tapioca.

- If an app isn’t listed:
  - It was not tested
  - Automation did not trigger HTTPS network traffic
  - It is not vulnerable
Issues Encountered

So you’ve got a million APK files?
Windows CMD.EXE
Windows CMD.EXE
THANKS MICROS~1  !!!1!
8.3 Filenames

“Note: Although disabling 8.3 file name creation increases file performance under Windows, some applications (16-bit, 32-bit, or 64-bit) may not be able to find files and directories that have long file names.”

http://support.microsoft.com/kb/121007
Busybox

- **recursive_action (and thus find) slow due to [l]stat()**

Conceptually, the find utility need not perform lstat on each filename unless it's needed for matching criteria. However, find is implemented based on libbb's recursive_action, which always performs stat or lstat. This makes busybox's find excruciatingly slow compared to GNU find.
Solution

- Real fileserver with ZFS.
You keep using that word. I do not think it means what you think it means.
How to track Vulnerabilities?

- CVE is the de facto standard for tracking vulnerabilities in applications.
- MITRE, who operates CVE, does not attempt to track all applications with CVE.
What Makes an App Important?

5-10 million installs
Insecurely retrieves ads
No CVE assigned
What Makes an App Important?

1-5 installs
Insecurely uses paypal
No CVE assigned
What Makes an App Important?

- 5-10 million installs
- Sends user/password
- No CVE assigned
CVE10K

We released 5-digit CVE-2014-10001 and 6-digit CVE-2014-100001 IDs on January 13, 2015, plus 90 others. Issues, compliments, or concerns welcome.

Everywhere

@cve.mitre.org/cve/identifier...

Tweet to CVE10K
CVE Assignment

- Are Android applications CVE-worthy?
CVE Assignment

- Are Android applications CVE-worthy?

- No*  

* Maybe, but stop assigning CVEs
What Makes an Android Developer?

A pulse
Create an Android App for FREE!

We have 986,081,580 installed Apps & 1,458,468 created Apps, 4,147,483,647 ads served

CREATE NOW!

Now AppsGeyser is turning app development into something that literally anyone can do" - The Next Web
AppsGeyser

- BROWSER STYLE
- ADD HOMEPAGE LINKS
- CUSTOMIZE YOUR BROWSER

APP NAME
App name needs to stand out so that people will download.

Ag cert test

Browser name examples:
- 4G Fast Internet Browser
- Speed Up Internet Browser
- Super Fast Browser

Click here to see the preview
Vulnerability Note VU#1680209

AppsGeyser generates Android applications that fail to properly validate SSL certificates

Original Release date: 19 Dec 2014 | Last revised: 07 Jan 2015

Overview

AppsGeyser generates applications that fail to properly validate SSL certificates.

Description

AppsGeyser is an online tool that generates Android applications. At the time of publication of this vulnerability note, the AppsGeyser website claims to have generated over 1.3 million Android applications. The applications that are generated by AppsGeyser include code that disables SSL certificate validation for HTTPS traffic.
AppsGeyser Fixed

Impact
When a victim is using an application generated by AppsGeyser, an attacker on the same network as the Android device may be able to view or modify network traffic that should have been protected by HTTPS. The impact varies based on what the application is doing. Possible outcomes include credential stealing or arbitrary code execution.

Solution
Regenerate affected Android applications

The AppsGeyser application generator has been updated to correctly validate SSL certificates. Any applications that were created before December 24, 2014 should be regenerated.

Vendor Information (Learn More)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Status</th>
<th>Date Notified</th>
<th>Date Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppsGeyser</td>
<td>Affected</td>
<td>12 Dec 2014</td>
<td>19 Dec 2014</td>
</tr>
<tr>
<td>App Name</td>
<td>Domain Name</td>
<td>Category</td>
<td>Downloads</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------</td>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Fred Fuller Oil &amp; Propane</td>
<td>com.wFredFuller</td>
<td>Business</td>
<td>100+</td>
</tr>
<tr>
<td>Free 2 Browse</td>
<td>com.wFree2Browse</td>
<td>Tools</td>
<td>10+</td>
</tr>
<tr>
<td>Free Classifieds Pensacola</td>
<td>com.wFreeAds</td>
<td>Shopping</td>
<td>100+</td>
</tr>
<tr>
<td>Free Animations Sharing</td>
<td>com.wFreeAnimationsSharing</td>
<td>Entertainment</td>
<td>1,000+</td>
</tr>
<tr>
<td>Freebies Junction</td>
<td>com.wFreebiesJunction</td>
<td>Social</td>
<td>100+</td>
</tr>
<tr>
<td>FREE Binary Options Signals</td>
<td>com.wFREEBinaryOptionsSignals</td>
<td>Finance</td>
<td>1,000+</td>
</tr>
<tr>
<td>FREE Binary Options Strategy</td>
<td>com.wFREEBinaryOptionsStrategy</td>
<td>Finance</td>
<td>1,000+</td>
</tr>
<tr>
<td>Free Career Advice</td>
<td>com.wFreeCareerAdvisor</td>
<td>Business</td>
<td>100+</td>
</tr>
<tr>
<td>FREE COPIER SUPPORT COMMUNIT</td>
<td>com.wFREECOPYERSUPPORT</td>
<td>Tools</td>
<td>1,000+</td>
</tr>
<tr>
<td>FREE Craft and Hobby KINDLES</td>
<td>com.wFREECraftandHobbyKINDLEBOOKS</td>
<td>Books &amp; Reference</td>
<td>1,000+</td>
</tr>
<tr>
<td>REMOVED</td>
<td>com.wFreeCreditMonitoringTarget</td>
<td>REMOVED</td>
<td>REMOVED</td>
</tr>
<tr>
<td>Freedom</td>
<td>com.wFreedom1</td>
<td>News &amp; Magazines</td>
<td>10+</td>
</tr>
<tr>
<td>FreedomOutpost</td>
<td>com.wFreedomOutpost</td>
<td>News &amp; Magazines</td>
<td>100+</td>
</tr>
<tr>
<td>Freedom Wireless</td>
<td>com.wFreedomWireless1</td>
<td>Shopping</td>
<td>1,000+</td>
</tr>
<tr>
<td>EURUSD Forex Trading Signals</td>
<td>com.wFREEEURUSDForexTradingSignals</td>
<td>Finance</td>
<td>1,000+</td>
</tr>
<tr>
<td>FREE Forex Signals</td>
<td>com.wFREEForexSignals</td>
<td>Finance</td>
<td>10,000+</td>
</tr>
<tr>
<td>FREE GBPUSD Trading Signals</td>
<td>com.wFREEGBPUSDTradingSignals</td>
<td>Finance</td>
<td>500+</td>
</tr>
<tr>
<td>Free Gift Cards Palace</td>
<td>com.wFreeGiftCardsPalace</td>
<td>Shopping</td>
<td>1,000+</td>
</tr>
<tr>
<td>Free Hermes Bag- Get yours now</td>
<td>com.wFreeHermesBag</td>
<td>Shopping</td>
<td>500+</td>
</tr>
<tr>
<td>Latest Hindi Ringtone Free</td>
<td>com.wFreeHindiMovieLatestRingtone</td>
<td>Music &amp; Audio</td>
<td>10,000+</td>
</tr>
<tr>
<td>Free Insta Likes And Followers</td>
<td>com.wFreeInstaFollowersAndLikes</td>
<td>Social</td>
<td>500+</td>
</tr>
<tr>
<td>Free Keywords Suggestion Tool</td>
<td>com.wFreeKeywordsSuggestionTool</td>
<td>Tools</td>
<td>100+</td>
</tr>
<tr>
<td>Freelanced</td>
<td>com.wFreelanced</td>
<td>Business</td>
<td>100+</td>
</tr>
<tr>
<td>Credit Union</td>
<td>URL</td>
<td>Category</td>
<td>Downloads</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------</td>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Apex Federal Credit Union</td>
<td>com.metova.cuae.afcu</td>
<td>Finance</td>
<td>100+</td>
</tr>
<tr>
<td>ATL Federal Credit Union</td>
<td>com.metova.cuae.atlfcu</td>
<td>Finance</td>
<td>100+</td>
</tr>
<tr>
<td>Bloomington Postal ECU App</td>
<td>com.metova.cuae.bloomingtonpostal</td>
<td>Finance</td>
<td>10+</td>
</tr>
<tr>
<td>Community Credit Union Mobile</td>
<td>com.metova.cuae.ccu</td>
<td>Finance</td>
<td>500+</td>
</tr>
<tr>
<td>Day Air Credit Union</td>
<td>com.metova.cuae.dayair</td>
<td>Finance</td>
<td>1,000+</td>
</tr>
<tr>
<td>Education Personnel FCU</td>
<td>com.metova.cuae.educationpersonnel</td>
<td>Finance</td>
<td>100+</td>
</tr>
<tr>
<td>Enrichment Federal CU</td>
<td>com.metova.cuae.efcu</td>
<td>Finance</td>
<td>1,000+</td>
</tr>
<tr>
<td>Forest Area FCU Mobile</td>
<td>com.metova.cuae.fafcu</td>
<td>Finance</td>
<td>500+</td>
</tr>
<tr>
<td>Farm Bureau Family CU</td>
<td>com.metova.cuae.fbfcu</td>
<td>Finance</td>
<td>50+</td>
</tr>
<tr>
<td>Gulf Coast Educators FCU</td>
<td>com.metova.cuae.gcefcu</td>
<td>Finance</td>
<td>1,000+</td>
</tr>
<tr>
<td>GeoVista Credit Union Mobile</td>
<td>com.metova.cuae.gyvcu</td>
<td>Finance</td>
<td>1,000+</td>
</tr>
<tr>
<td>Honor Credit Union Mobile</td>
<td>com.metova.cuae.hcu</td>
<td>Finance</td>
<td>1,000+</td>
</tr>
<tr>
<td>La Terre Federal Credit Union</td>
<td>com.metova.cuae.laterrefcu</td>
<td>Finance</td>
<td>100+</td>
</tr>
<tr>
<td>Magnify Credit Union</td>
<td>com.metova.cuae.magcu</td>
<td>Finance</td>
<td>100+</td>
</tr>
<tr>
<td>Mountain Credit Union</td>
<td>com.metova.cuae.mcuc</td>
<td>Finance</td>
<td>1,000+</td>
</tr>
<tr>
<td>Memorial Credit Union Mobile</td>
<td>com.metova.cuae.memorial</td>
<td>Finance</td>
<td>500+</td>
</tr>
<tr>
<td>Notre Dame FCU</td>
<td>com.metova.cuae.ndfcu</td>
<td>Finance</td>
<td>1,000+</td>
</tr>
<tr>
<td>Partnership Financial CU</td>
<td>com.metova.cuae.ntscu</td>
<td>Finance</td>
<td>100+</td>
</tr>
<tr>
<td>Oak Trust CU App</td>
<td>com.metova.cuae.oaktrustcu</td>
<td>Finance</td>
<td>100+</td>
</tr>
<tr>
<td>Postal Family FCU App</td>
<td>com.metova.cuae.postalfamily</td>
<td>Finance</td>
<td>100+</td>
</tr>
</tbody>
</table>
Apps That Exist
And also fail to validate SSL
**Mobile Network Signal Booster**

**Description**

Mobile Network Signal Booster allows you to optimize the level of the signal in your phone and use the nearest stations to significantly improve signal reception and the Internet!

- Optimizes signal your phone in one click.
- Very easy-to-use
- Optimizes signal not only a phone, but also the work of the Internet in your handset.
- For more effective optimization it is recommended to repeat optimization for several days.

**Reviews**

Amazing Out of the multitude of apps that I have tried to strengthen my network signal, this is the only one that worked.

Nanci M. LambCranford ★★★★★

Wooow! Idk if this app really works for the evo 4g when I'm outside my house in the open area my signals fine with it.

Anthony Kasowski ★★★★★
# Mobile Network Signal Booster

## Additional information

<table>
<thead>
<tr>
<th>Updated</th>
<th>Size</th>
<th>Installs</th>
<th>Current Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 25, 2013</td>
<td>13M</td>
<td>50,000 - 100,000</td>
<td>1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requires Android</th>
<th>Content Rating</th>
<th>Contact Developer</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2 and up</td>
<td>Everyone</td>
<td>Email Developer</td>
</tr>
</tbody>
</table>
Cartoon Wars

Cartoon Wars
GAMEVIL Inc. - August 26, 2014
Arcade

Install  Add to Wishlist

This app is compatible with all of your devices. Offers in-app purchases

4.7 (469,875)
Top Developer

Google+  Recommend this on Google

CERT
Carnegie Mellon

RSAConference2015
# Cartoon Wars

## Additional information

<table>
<thead>
<tr>
<th>Updated</th>
<th>Size</th>
<th>Installs Range</th>
<th>Current Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 26, 2014</td>
<td>15M</td>
<td>10,000,000 - 50,000,000</td>
<td>1.1.1</td>
</tr>
</tbody>
</table>

**Requires Android**
- 2.2 and up

**Content Rating**
- Medium Maturity

**In-app Products**
- $0.99 - $99.99 per item

**Permissions**
- View details

**Report**
- Flag as inappropriate

**Offered By**
- GAMEVIL Inc.

**Developer**
- Visit Website
- Email
- contact@gamevilusa.com
- Privacy Policy
- 999 N Sepulveda Blvd, Ste 150, El Segundo, CA, United States
Cartoon Wars

Superuser Request

Cartoon Wars is requesting Superuser access.

Warning: If you do not understand this, you should deny the request.

Cartoon Wars

Developer Warning: android.permission.ACCESS_SUPERUSER not declared in manifest.

- This time only
- Remember choice for 10 minutes
- Remember choice forever

Deny | Allow
Brightest LED Flashlight

Brightest LED Flashlight
Intellectual Flame Co., Ltd. - September 2, 2014
Tools

Install Add to Wishlist

This app is compatible with all of your devices.

☆☆☆☆☆ (★575,802)

+141458 Recommend this on Google

Software Engineering Institute
Carnegie Mellon

CERT

RSA Conference 2015
Selected Developer Responses

Still optimistic?
Hello,

Thank you for your e-mail! The app that you have in mind is not created or related to us or [REDACTED]. We recently found out about it and we are looking for a way to take it down as it's made by a person trying to exploit [REDACTED]'s name. Is there a way to report this app and take it down? We would really appreciate help in this.
Application author response

I understand, i was consuming a service the generates real random numbers based on measurements of quantum phenomena.

So i just didnt cared about the ssl config on the http request since it was a very trivial.
I don't know what the hell you're talking about, my application does not include any SSL connection !!!
Application author response

Remove
Application author response

What????
Application author response

I want to thank you very much fix for SSL, but Google Play Store my suspends, I want to fix bugs, I want to get back my application, please help
Application author response

Mr. Will

Thanks alot for your analysis. We checked everything in the app. There is not even a single bug. Your mail is type a type of spam which is of no use. If you really have something then work practically.
Hi CERT Coordination Center,

Our application is an authentication application and has among other features a backend where there is a Risk Engine present, the communication taking place when connecting with a faulty certificate is to merely a notification mechanism to tell the server the communication channel is being tampered with. As such, it is a feature that our application to continue to communicate with the backend even even thought the channel is compromised by usage of a faulty certificate.
Application author response

Well I’m not sure how a SSL Vulnerability can be present in an application when I don’t take any payments through the application for any product. Looks like you have much more testing to do. Can you please stop sending me emails.

Thanks

—
Application author response

take me off your list
Application author response

Please contact the NSA.gov for this case because I am not the owner of this site

Thank you
Public Reception
Fighting the battle of who could care less
I've got a security notice about a SSL vulnerability in my (very simple) app. It's spam, right? (self.androiddev)

submitted 1 day ago * by wowsuchlinuxkernel

I get tons of those mails, and I usually do recognise what's spam and what is not. Just for fun, I checked the files attached to the mail (it's a text file and I run Linux) and found the classes of my app that connect to the internet in it, seeming as if it was real. The mail is from cert@cert.org, but the sender email is very easy to fake.

Should I be concerned?

Edit: There are three files attached, one containing the classes that connect to the internet, one with a few URLs (that apparently have been used for the MITM attack) and one binary file that I am still failing to open:

```
username@hostname /tmp $ mitmproxy -r abc.def.ghi.apk.flows.log.bin
warning: You are using mitmproxy 0.10.1 with netlib 0.11.1. Most likely
Traceback (most recent call last):
 File "/usr/bin/mitmproxy", line 36, in <module>
   config = proxy.process_proxy_options(parser, options)
 File "/usr/lib/python2.7/site-packages/libmproxy/proxy.py", line 590
certutils.dummy_ca(cacert)
AttributeError: 'module' object has no attribute 'dummy_ca'
```
The issue would be that if you do not use SSL somebody using your app who is on a hostile network could have that publicly available file replaced with a malicious file without realizing it. The replacement could be filled with phishing links or exploit a vulnerability in the code that is processing that file.

[-] flagrantaroma  4 points 1 day ago

Right! Thanks, I did not think about that. My app's audience are people who have much knowledge of computers so I think I can keep this "bug" unfixed.

Thank you for your help.

[-] wowsuchlinuxkernel  [S] -8 points 1 day ago
I just received email from CERT Coordination Center, I don't know what is happen ????

Yeah I had one of these for an app that gets hardly any downloads. I don't think their affiliated with Google though and the e-mail seems quite arbitrary anyway. No big deal if you ask me.

Sign up with mobileCore here for $100 bonus when reaching 100k impressions!
AttractiveInterstitial Ads (and other ad units) that perform well in both apps in games and on a global scale. Weekly payments too!

Sign up with StartApp here for $15 when you hit 100k ad impressions!
They run a great range ofInterstitial Ads for apps and games on a global scale, with banners available too.

DO NOT USE inMobi. Check out this thread.

I also got one yesterday. I ignore it unless it is sent by google.
Twitterverse #1 (warmup)

Will Dormann @wdormann · Sep 27
I like it when apps tell me that everything is going to be OK.
Thanks, CM Browser!

docs.google.com/spreadsheets/d...
pic.twitter.com/02kPkDTQbK
Four Months Later

Still Vulnerable
Coles Supermarkets
@Coles

@wdormann privacy & security is of the upmost importance to us & our credit card app has never experienced a security vulnerability.
Reality-distortion field

“We have systems in place to immediately react to the ever-changing demands of the digital environment. Our credit card app has never experienced a security vulnerability.”

The spokesperson added that the app is read only and all customer’s money is protected under MasterCard’s guarantee.

Let’s go nuclear
Vendor Reaction
Not Everything is Bad

At least one
Hello.

Thank you very much for the reply. I've confirmed that our record has been updated in the spreadsheet. And let me say thank you again for your hard efforts to investigate and report problems in large number of Android apps. Without your help, we'd have overlooked the issue much longer.

Best Regards,
Statistics
Numbers don’t lie?
The Numbers

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free Apps Tested</td>
<td>1,000,500</td>
<td>Most?</td>
</tr>
<tr>
<td>Vulnerable Apps Discovered</td>
<td>23,667</td>
<td>2.4%</td>
</tr>
<tr>
<td>Vulnerable App Authors Notified</td>
<td>23,301</td>
<td>98.5%</td>
</tr>
<tr>
<td>Email responses</td>
<td>1,593</td>
<td>6.8%</td>
</tr>
<tr>
<td>Email responses with fix details</td>
<td>25</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

“There are now 1 million apps in the Google Play store.”
July 24, 2013

http://mashable.com/2013/07/24/google-play-1-million/
Where do we go from here?

Forward
Further Work

- Full SSL visibility (Root CA cert installed)
- Improved automation
- Other Platforms (IOS, Blackberry, Windows Phone)
- True Scalability
Conclusions

- Vulnerability coordination doesn’t scale easily
- CVE doesn’t scale easily
- There are plenty of horrible Android applications
- Application authors aren’t very responsive
Apply What You Have Learned Today

- Next week you should:
  - Download CERT Tapioca
  - Test using CERT Tapioca

- In the first three months following this presentation you should:
  - Use Tapioca to test applications used in your organization for SSL validation failures
    - Non-free applications
    - Non-Android applications
    - Report failures to CERT