



Flash Update

Dec. 17, 2015

Leader: Rhudolf Valentin Flores

Members: Tristan Jhorme Sigue

Christian Jesse Tragico

Vince Anthony King Ayende

COMSEC2 – Project Documentation

Vulnerability Found: AVM Bytecode Verification

Main Source: ADOBE FLASH PLAYER

Vulnerability Type: `_X_SYSTEM`

Background of the Study

What is Adobe Flash Player?

Adobe Flash Player is the standard for delivering high-impact, rich Web content, Designs, animation, and application user interfaces are deployed immediately across all browsers and platforms, attracting and engaging users with a rich Web experience.

What is the AVM Bytecode Verification Vulnerability?

This module exploits a vulnerability in Adobe Flash Player versions 10.2.152.33 and earlier. This issue is caused by a failure in the ActionScript3 AVM2 verification logic. This results in unsafe JIT(Just-In-Time) code being executed. This is the same vulnerability that was used for the RSA attack in March 2011. Specifically, this issue results in uninitialized memory being referenced and later executed. Taking advantage of this issue relies on heap spraying and controlling the uninitialized memory. Currently this exploit works for IE6, IE7, and Firefox 3.6 and likely several other browsers. DEP does catch the exploit and causes it to fail. Due to the nature of the uninitialized memory it's fairly difficult to get around this restriction.

Affected System Version/s:

- Adobe Flash Player 10.2.152.33 and earlier versions for Windows, Macintosh, Linux and Solaris
- Adobe Flash Player 10.2.154.18 and earlier for Chrome users
- Adobe Flash Player 10.1.106.16 and earlier versions for Android
- Adobe Reader and Acrobat X (10.0.1) Earlier 10.x and 9.x versions of Reader and Acrobat for Windows and Macintosh

Solution/s:

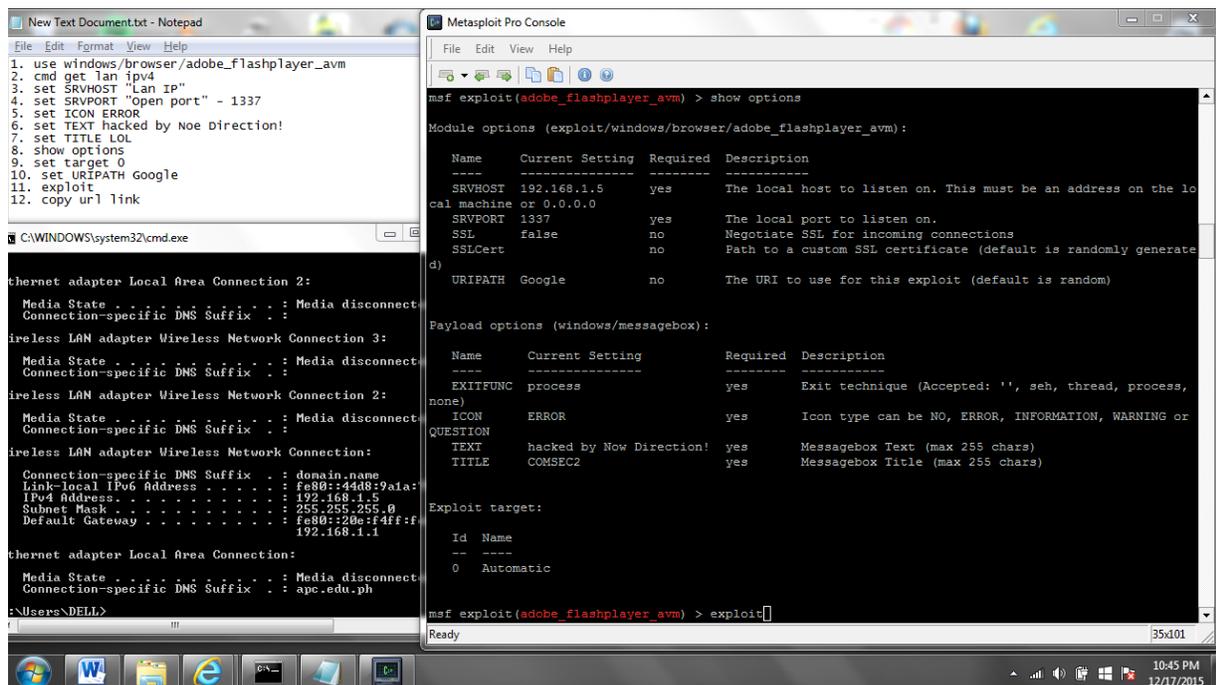
1. Upgrade your Adobe Flash Playerto the latest version of Adobe Flash Player (version 11.2 or later).
2. Always check for Adobe Flash Player notification security check and updates at least once a week.
3. Install and uninstall the software safely to ensure that the software has not infected and has no virus.

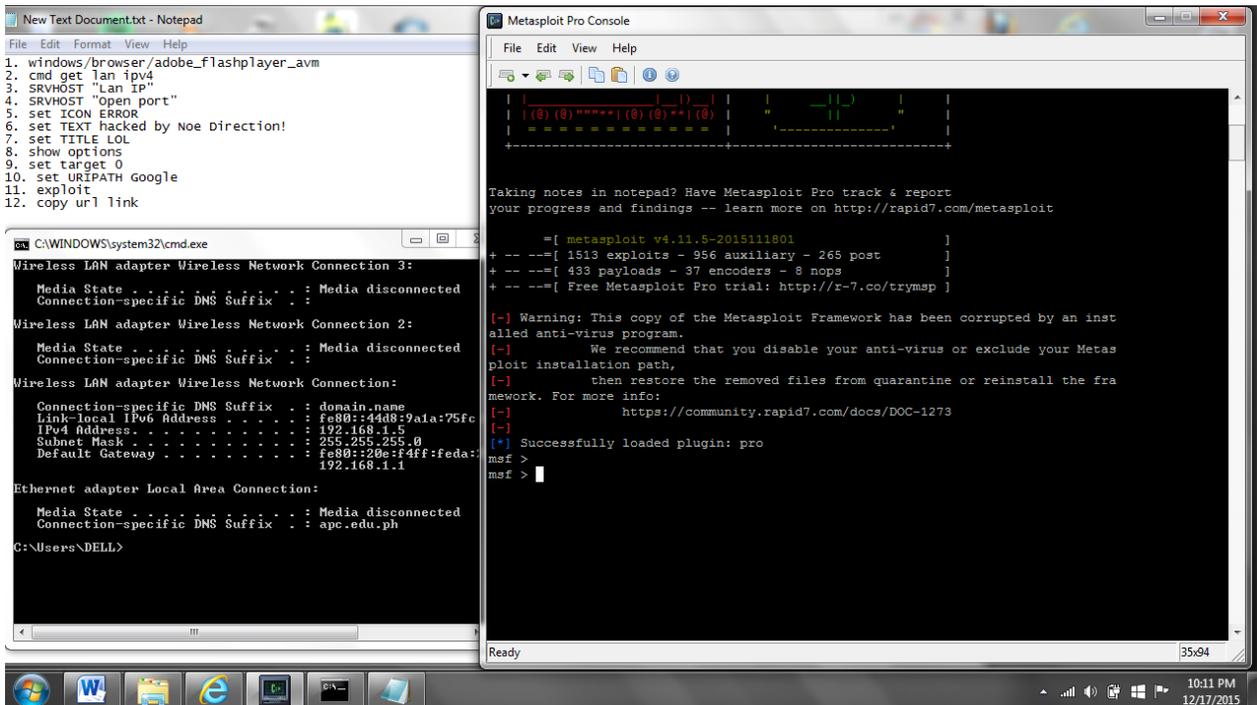
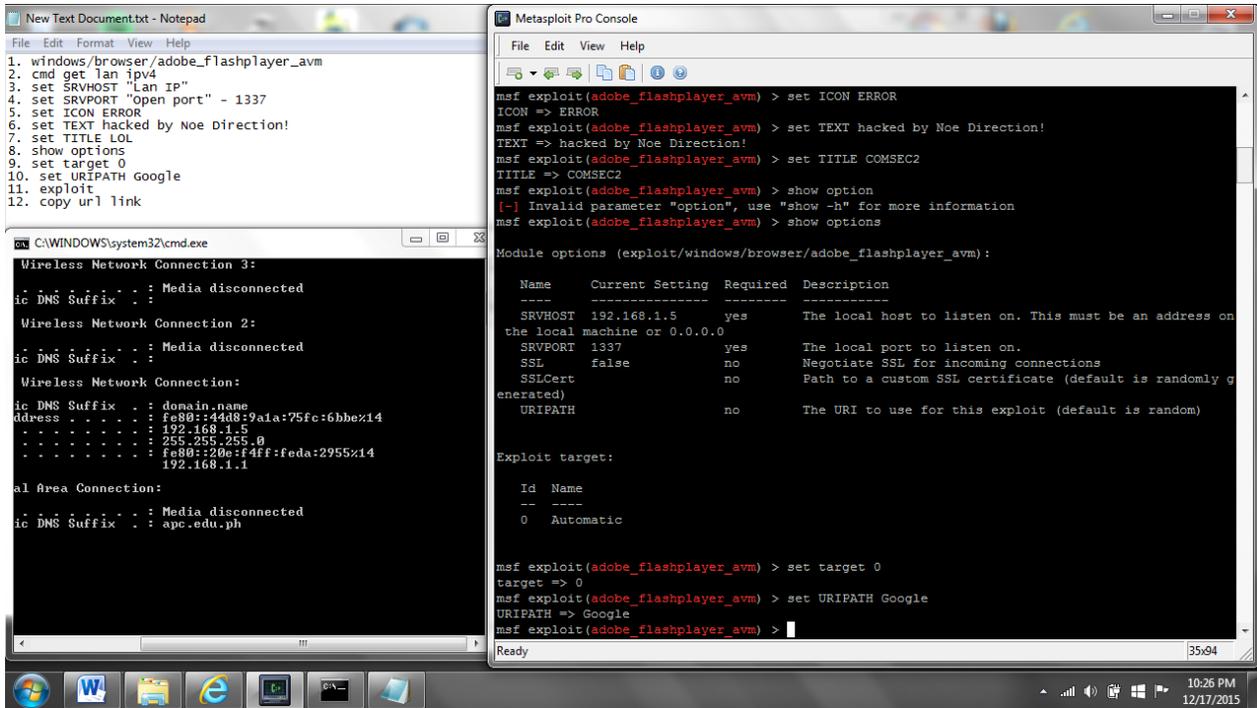
Vulnerability Testing

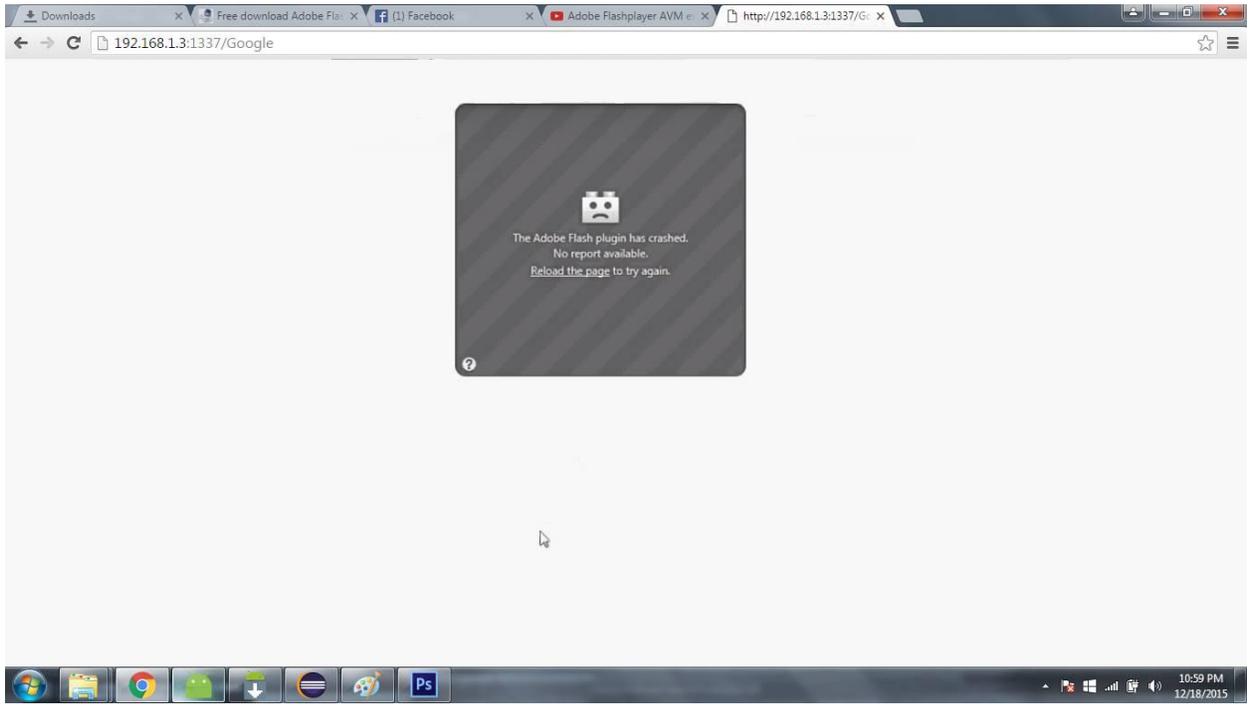
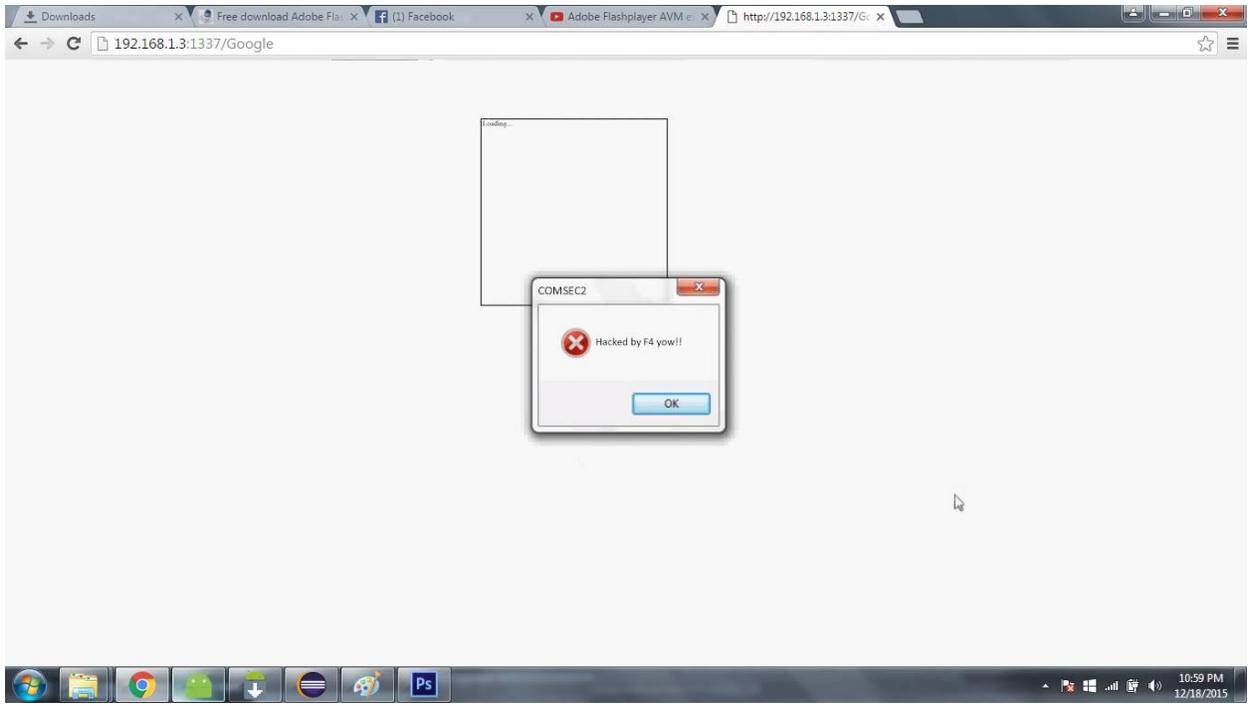
Technologies, programs, and languages used in demo testing:

- Laptop (Microsoft Windows OS)
- Virtual Machine (Microsoft Windows OS)
- Command Prompt window (cmd)
- Third party software (Metasploit)
- Internet Browser

Screenshots







Conclusion/s:

Our group has therefore concluded that the Adobe Flash Player can be vulnerable to attacks and that you should always keep your version up to date to minimize the chance of attackers to victimize your computer. But Even though your Adobe Flash Player has been already updated the exploit are still working but not completely executed or done because Adobe has already fix that vulnerability has been found in the older version of their flash player.

Reference/s:

<http://eromang.zataz.com/2011/03/27/cve-2011-0609-adobe-flash-player-avm-bytecode-verification-vulnerability/>

https://www.rapid7.com/db/modules/exploit/windows/browser/adobe_flashplayer_avm

https://www.youtube.com/watch?v=8MX_fH4wCEQ – AVM Exploit