Vulnerability Report for CVE-2016-4117

CVE-2016-4117 CVSS Scores & Vulnerability Types	
CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
Platforms Affected	Windows, Macintosh, Linux and Chrome OS [1]

- A basic description of the vulnerability and how it can be exploited.

A critical vulnerability (CVE-2016-4117) exists in Adobe Flash Player 21.0.0.226 and earlier versions for Windows, Macintosh, Linux, and Chrome OS. Successful exploitation could cause a crash and potentially allow an attacker to take control of the affected system [2].

Consider you received an email containing a MS Office document from someone or you downloaded a MS Office document hosted on DDNS server. If this MS Office document is specially crafted by the attacker who intend to exploit this vulnerability, then following actions will possibly happen.

1. You open the MS Office Document on a system which runs Flash Player 21.0.0.226 or earlier but not older than 21.0.0.196 [6]
2. You will see the flash based content in the document and exploit is triggered
3. Your computer connects to an attacker's server and downloads malicious payload
4. You will see a decoy document and might not recognize anything malicious but your system is compromised and it is possibly part of a Botnet waiting for the instructions from Command and Control (C&C) server [Please see technical detail section for more information]

- What systems are impacted?

All Windows, Macintosh, Linux and Chrome OS platforms running Adobe Flash Player 21.0.0.226 or earlier are impacted by CVE-2016-4117 vulnerability.

- What can be done to mitigate against the vulnerability?

Adobe addressed CVE-2016-4117 on May 12, 2016 and recommended users to update their product installation to the latest versions using the instructions referenced in the security bulletin [2]. Additionally, users can also avoid using Adobe Flash Player if it is not required for their systems

- Is exploit code available?

Yes. There is no Metasploit module for CVE-2016-4117 but following steps can be followed in order to read out and write arbitrarily in memory

1. Attacker defines a property name like "placement" that conflicts with the inner interface name in com.adobe.tvsdk.mediacore.timeline.operations.DeleteRangeTimelineOperation
2. Now call to the "placement" interface causes the ActionScript VM to call internal function getBinding to get bind id
3. As the property "placement" is conflicting with the interface name, the attacker can manipulate the bind id and create conflict
4. In order to introduce shell code to control memory the exploit defines object that extends ByteArray with distinguished values. The distinguished values aid the exploit in locating the objects in memory easily
5. The "placement" property now can manipulate the bind id to read out of bound and point to the extended ByteArray which contains shell code
6. As the shell code present in the ByteArray is getting executed the attacker has ability to corrupt one of the objects to extend its length to 0xffffffff (high memory) and its data buffer to address 0 i.e. the object is capable of reading and writing all the content of the memory (RAM)
7. As an example if the system is a web server the private key value stored in the memory can be read by the exploit and compromise the web server's identity [3]

- How could exploitation activities impact vulnerable systems?

Consider that the underlying system is Ubuntu based web server running Adobe Flash Player version 21.0.0.226 or earlier but not older than 21.0.0.196.
As explained in earlier section the successful exploit allows attacker to read and write the content of the memory. There are many different types of system compromises possible. Some of the possible compromises are listed below

1. Attacker acquiring all the content of the memory and sending it over to C&C servers
2. Attacker flushing the memory which could cause interruption to some of the services or crashing of programs
3. Attacker installing backdoor so that compromised host can be accessed in future
4. Attacker extracting sensitive information like private keys, passwords (possible in some cases)
5. Attacker running strace or debugger utility to attach to the running process to find the possible system calls/ variables and changing the values of system calls/ variables
6. Attacker taking complete control of the system and destroying system completely

Reference:
[1] http://www.cvedetails.com/cve/CVE-2016-4117/
[2] https://helpx.adobe.com/security/products/flash-player/apsa16-02.html
[3] https://www.fireeye.com/blog/threat-research/2016/05/cve-2016-4117-flash-zero-day.html
[4] https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-8-adds-support-for-flash-vulnerability
[5] http://malware.dontneedcoffee.com/2016/05/cve-2016-4117-flash-up-to-2100213-and.html
[6] http://blog.morphisec.com/flash-vulnerability-cve-2016-4117