Security vulnerabilities in software from major IT companies have exposed systems to external attacks and malicious software, leading to significant security risks and potential data breaches. Adobe, like many other prominent companies, has faced such vulnerabilities, highlighting the importance of robust security practices. In this context, we will highlight two notable security issues that emerged in 2015 and 2016, particularly concerning Adobe Flash Player. Notably, the vulnerability discovered in 2015 was classified as critical and posed a severe threat to user systems. Both of these issues were subsequently identified, patched, and addressed in later software updates and versions, emphasizing the need for continuous vigilance in maintaining secure software environments.

Software Vulnerabilities

Report on known vulnerabilities:

Adobe Flash Player

CVE-2015-7645 | CVE-2016-7855

OpenSSL

CVE-2015-7645 | CVE-2016-7855

a). On October 14, 2015, Adobe issued a security bulletin (APSA15-15) regarding a critical vulnerability identified as CVE-2015-7645. This vulnerability impacted Adobe Flash Player version 19.0.0.207 and later on platforms including Windows, Macintosh, and Linux. The severity of this vulnerability was significant, as its successful exploitation could cause system malfunction and potentially allow an attacker to gain control of the affected system.

Affected Software Versions:

- Adobe Flash Player 19.0.0.207 and later for Windows and Macintosh
- Adobe Flash Player Extended Support Release (ESR) version 18.0.0.252

  and later in the 18.x series

- Adobe Flash Player 11.2.202.535 and later in the 11.x series for

  Linux systems

Adobe then recommended that users verify the version of the software running on their systems, providing instructions for this process. If users utilize multiple browsers, the check should be performed separately for each browser.

A **Zero-Day Exploit** refers to a cyber attack that occurs on the same day a vulnerability is discovered in software, before the vendor has a chance to release a patch or solution. In this case, the vulnerability was exploited by the **Pawn Storm** group, also known as APT28, Sednit, Fancy Bear, Sofacy, and Tsar Team. This group, active in cyberattacks since 2007, targeted various Ministries of Foreign Affairs globally, as well as NATO and the White House. Using **phishing** techniques, the attackers deceived users through email, and once successful, they installed **Sednit**-type malware on the victims' systems. This allowed the attackers to take control of the machines, leak documents, and cause significant damage or even complete system takeover.

The vulnerability, **CVE-2015-7645**, was discovered by Peter Pi of Trend Micro, who reported the issue and collaborated with the company to protect its customers. Additionally, **Google's** Natalie Sivanovich assisted in analyzing and resolving the vulnerability.

The problem was fixed immediately the next day - October 16th2015.

CVE-2015-7645 | **CVE-2016-7855**

On October 26, 2016, Adobe released a security update for Flash Player that addressed a significant vulnerability identified as APSB16-36, with a priority rating of 1. This vulnerability affected platforms including Windows, Macintosh, Linux, and Chrome OS. Classified as critical, it posed a serious risk, as an attacker could potentially gain control of the affected systems.

Product Affected Versions Platforms

Adobe Flash Player Desktop Runtime	23.0.0.185 and later Windows and Macintosh
Adobe Flash Player for Google Chrome	23.0.0.185 and later Windows, Macintosh, Linux and Chrome OS
Adobe Flash Player for Microsoft Edge and Internet Explorer 11	23.0.0.185 and later Windows 10 and 8.1 11.2.202.637 and later
Adobe Flash Player για Linux	23.0.0.185 and later Windows and Macintosh 23.0.0.185 and later Windows, Macintosh, Linux, and Chrome OS 23.0.0.185 and later Windows 10 and 8.1 11.2.202.637 and later

Adobe then provides instructions for identifying and verifying the version that users are running. If users use multiple browsers, then the check should be done for each browser installed on the system.

Solution:

Adobe categorizes upgrades and prompts users to install the latest version.

Product **Upgraded version** **Platform** **Priority** **Availability**

Product	Updated Versions	Platform	Priority rating
Adobe Flash Player Desktop Runtime	23.0.0.205	Windows and Macintosh	1
Adobe Flash Player for Google Chrome	23.0.0.205	Windows, Macintosh, Linux and Chrome OS	1
Adobe Flash Player for Microsoft Edge and Internet Explorer 11	23.0.0.205	Windows 10 and 8.1	1
Adobe Flash Player for Linux	11.2.202.643	Linux	3

The vulnerability, identified as **CVE-2016-7855**, was discovered by Neel Mehta and Billy Leonard from Google's Threat Analysis Team. The researchers confirmed that the vulnerability was actively being exploited in targeted attacks against users running **Windows 7, 8.1, and 10**.

CVE-2015-7645 | CVE-2016-7855

b). According to the organization: CVE
At the address: http://cve.mitre.org/

Adobe Flash Player versions **18.x** (up to **18.0.0.252**) and **19.x** (up to **19.0.0.207**) on **Windows** and **Mac OS**, as well as **11.x** (up to **11.2.202.535**) on **Linux**, contained a known vulnerability that allowed remote attackers to execute arbitrary code via a specially crafted SWF file. This issue, which surfaced in **October 2015**, posed significant security risks.

The vulnerability in Adobe Flash Player versions prior to **23.0.0.205** on **Windows** and **Mac OS**, and prior to **11.2.202.643** on **Linux**, could allow remote attackers to execute arbitrary code via unspecified vectors. This vulnerability was actively exploited in **October 2016**.

According to the CVE database, there are **17 vulnerabilities** specifically associated with Adobe Flash Player. On **cvedetails.com**, a total of **2,533 Adobe vulnerabilities** were recorded between **1999 and 2018**. The highest number of vulnerabilities was reported in **2016**, with **548** in total. Of these, Adobe Flash Player accounted for the most vulnerabilities, with **1,048** reported across its versions.

c). According to the website: https://nvd.nist.gov
The severity of this vulnerability is 9.3

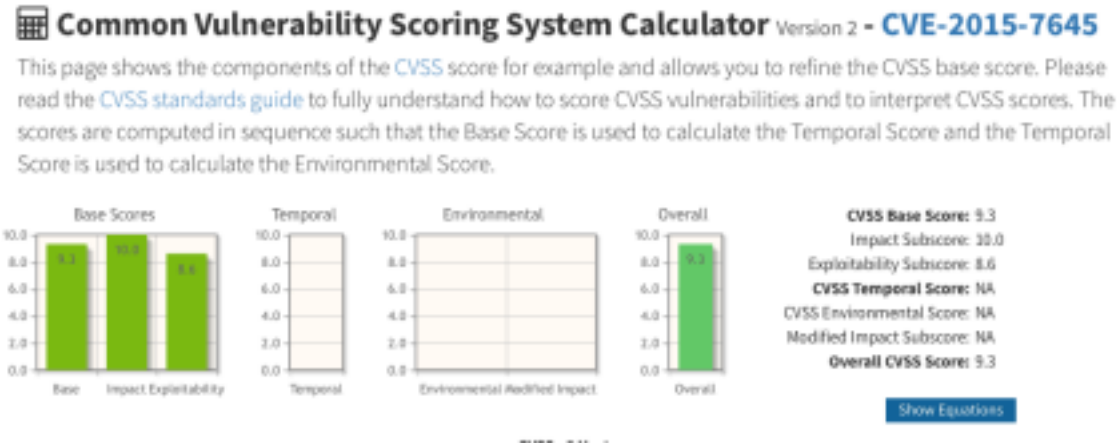

Figure 1.1

The graph shows the detailed way in which the severity rating is derived through the metrics applied

The severity of the vulnerability is rated 9.8 on Windows.

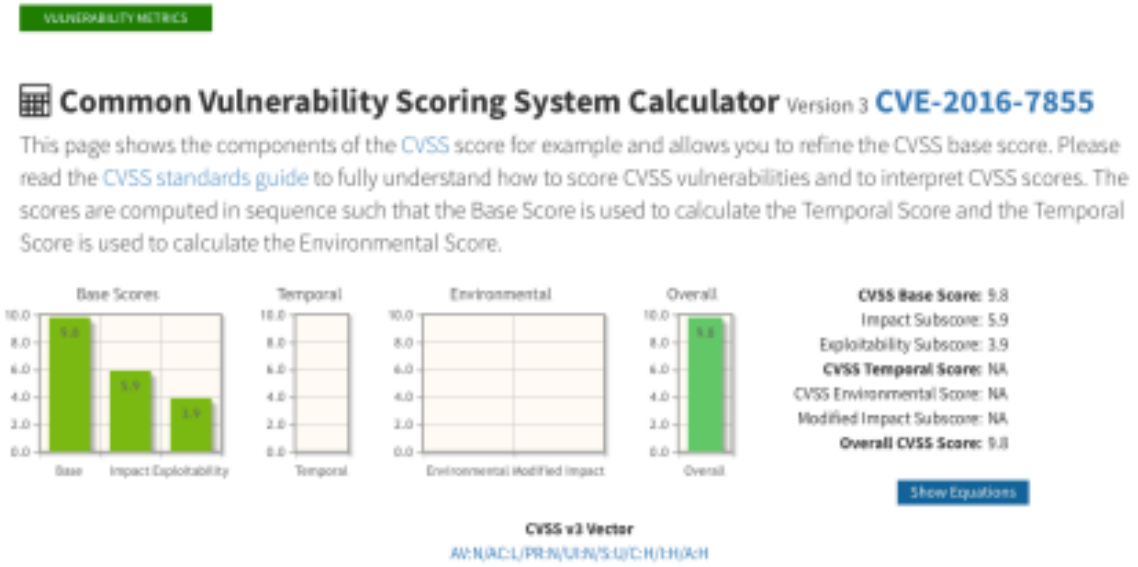

Figure 1.2

While on Linux operating systems with 10.

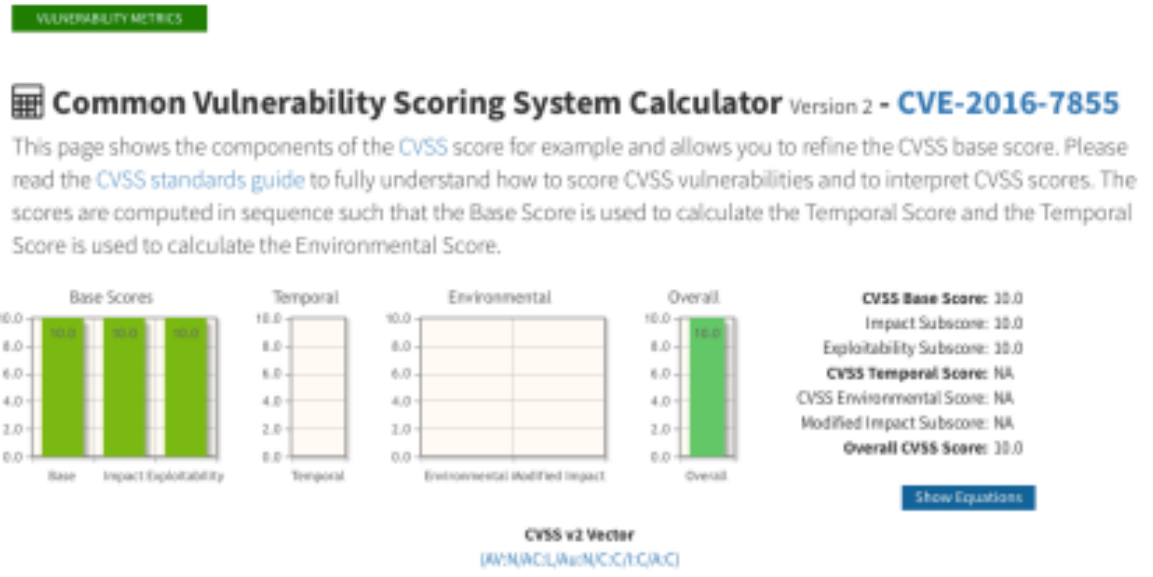

Figure 1.3

CVE-2015-7645 | CVE-2016-7855

d).The website **securityfocus.com** offers comprehensive details about these vulnerabilities, including information on the most stable versions of Adobe Flash Player that are not affected by these issues.

Not Vulnerable: **Adobe Flash Player 19.0.0.226**
Adobe Flash Player 18.0.0.255
Adobe Flash Player 11.2.202.540

CVE-2015-7645 **| CVE-2016-7855**

Accordingly, detailed information is provided for this vulnerability as well as two versions that do not present vulnerabilities.

Not Vulnerable: **Adobe Flash Player 23.0.0.205**
Adobe Flash Player 11.2.202.643

e).Known OpenSSL vulnerabilities:

I. 278 vulnerabilities have been identified from 2000 to 2018.
First reported: CVE-2000-1254
Latest: CVE-2018-0739

II. No information is provided regarding the severity of the vulnerability for this recent entry CVE-2018-0739.

Vuln ID	Summary	CVSS Severity
CVE-2018-0739	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n). **Published:** March 27, 2018; 05:29:00 PM -04:00	(not available)

Figure 2.1

III. For the vulnerability: CVE-2018-0739 the website: securityfocus.com It gives the following information:
Bug ID: 103518

Class: failure to handle Exceptional Conditions.
It concerned users who operated the system remotely and not those who operated on a local machine. It was published on March 27, 2018 and the update was made on the same day. The vulnerability was discovered by Matt Casswell.
Here is a list of the vulnerable versions:

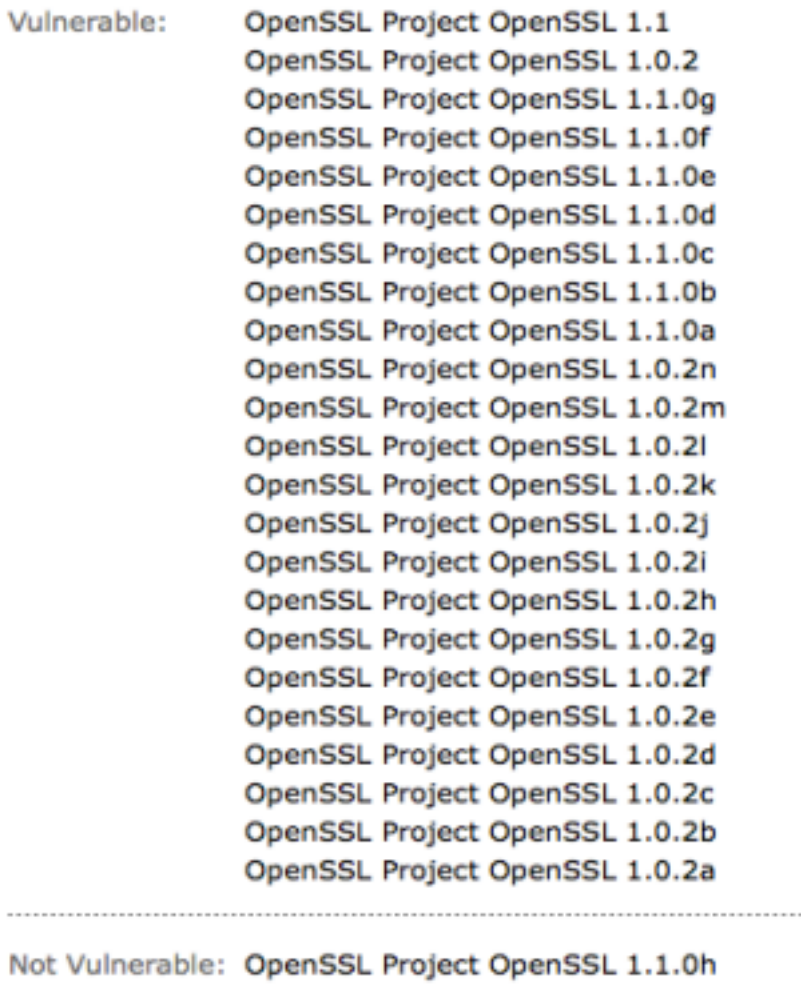

Figure 2.2

From the image we see the one and only version of OpenSSL OpenSSL 1.1.0h which is not among the vulnerable versions and is safe to use.

Sources of information used:

https://blog.trendmicro.com/trendlabs-security-intelligence/latest flash-exploit-used-in-pawn-storm-circumvents-mitigation techniques/

Ambel Basha
Athens 4 April 2018