Tugas

Keamanan Jaringan Komputer

Disusun Oleh :

Nama : Sigit Wijaya Pramono

NIM : 09011181419012

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

5 CVE *DoS* Attack in Apache

1. Vulnerability Details : CVE-2009-2412

Beberapa overvlow integer pada Apache Portable Runtime (APR) library memungkinkan para penyerang jarak jauh menyebabkan *Denial of Service (Aplication Crash)*. Berikut merupakan capture dari hasil pencarian CVE dari apache yang berisi banyak informasi :

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	Admin
Vulnerability Type(s)	Denial Of Service Execute Code Overflow

2. Vulnerability Details : CVE-2015-5343

Integer overflow di util.c di mod_dav_svn pada Apache Subversion 1.7.x, 1.8.x sebelum 1.8.15, dan 1.9.x sebelum 1.9.3 memungkinkan pengguna yang diautentikasi jauh menyebabkan *Denial of Service* (crash server subversion atau konsumsi memori) dan mungkin mengeksekusi kode sewenang-wenang via *a skel-encoded request body*, yang memicu *out-of-bounds read* dan *heap-based buffer overflow*. Selanjutnya merupakan capture dari hasil pencarian pada CVE details :

CVSS Scores & Vulnerability Types

CVSS Score	8.0
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
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	Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Execute Code Overflow
CWE ID	119

3. Vulnerability Details : CVE-2017-5661

Pada Apache FOP sebelum 2.2, file yang terdapat di filesystem server yang menggunakan FOP dapat diturunkan ke pengguna yang sewenang-wenang yang mengirim file SVG yang berdampak buruk. Jenis file yang dapat ditampilkan bergantung pada konteks pengguna dimana aplikasi yang dieksploitasi sedang berjalan. XXE juga dapat digunakan untuk menyerang ketersediaan server melalui *Denial of Service* karena referensi dalam dokumen xml dapat secara sepele memicu serangan amplifikasi. Berikut juga capture dari hasil pencarian pada cve details :

CVSS Scores & Vulnerability Types

CVSS Score	7.9
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	611

4. Vulnerability Details : CVE-2017-5662

Pada vulnerability CVE-2017-5662 ini hampir sama dengan vulnerability sebelumnya, terutama pada jenis kerentanan nya *(vulnerability type)* yaitu *Denial of Service*. Di Apache Batik sebelum 1.9, file yang tergeletak di filesystem server yang menggunakan batik dapat diungkap ke pengguna sewenang-wenang yang mengirim file SVG yang berdampak buruk. Berikut capture penjelasan nya :

CVSS Scores & Vulnerability Types

CVSS Score	7.9
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	611

5. Vulnerability Details : CVE-2002-2272

Tomcat 4.0 sampai 4.1.12, dengan menggunakan modul mod_jk 1.2.1 pada Apache 1.3 sampai 1.3.27, memungkinkan penyerang jarak jauh menyebabkan *DoS* (desynchronized communications) melalui permintaan HTTP GET dengan field Pengambilan Transfer Encoding dengan nilai yang tidak valid. Berikut ini captue penjelasan-penjelasannya :

CVSS Scores & Vulnerability Types

CVSS Score	7.8
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
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)	Denial Of Service Overflow
CWE ID	119

Analisa

Dalam lima rate CVE *(Common Vulnerabilities and Exposures)* tertinggi dari Apache yang di ambil diatas, dipilih angka rate, tahun, yang beragam. Dari lima jenis cve diatas setiap cve serangannya lebih mengarah ke *Denial of Service (DoS)*. Kerentanan satu sama lain hampir sama, dan beberapa diantaranya ada yang jenis kerentanannya *Denial of Service Execute Code Overvlow* yang kurang lebih sama dengan yang sebelumnya.