TUGAS
KEAMANAN JARINGAN KOMPUTER

Disusun Oleh :

Nama : Randa Fratelli Junaedi

NIM : 09011181419006

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

Common Vulnerabilities and Exposures (CVE)

Server HTTP Apache merupakan server web yang dapat dijalankan di banyak sistem operasi (Unix,BSD, Linux, Microsoft Windows dan Novell Netware serta platform lainnya) yang berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP.

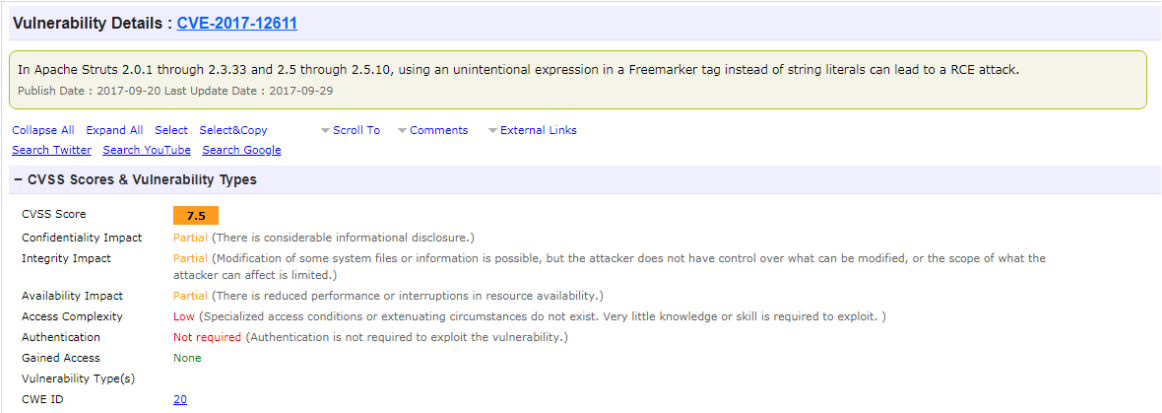
Cara kerja Server HTTP Apache seperti mesin dimana tempat aplikasi atau software beroperasi dalam medistribusikan web page ke user, tentu saja sesuai dengan permintaan user.

Di mana dalam tugas ini, penulis menggunakan suatu web server apache, dan contoh website berikut ini http://www.pusri.co.id/ina/home/ telah menggunakan web server apache, dimana cara untuk melihat website tersebut menggunakan sebuah website https://www.netcraft.com/.

Netblock owner	IP address	OS	Web server	Last seen
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.4.120	Linux	Apache/2.2.16 Debian	19-Feb-2018
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	-	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/5.2.5 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	25-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	unknown	24-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/5.2.5 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	22-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.4 OpenSSL/0.9.8d PHP/5.2.1 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	3-Oct-2007

CVE adalah daftar entri yang dimana masing-masing berisi nomor identifikasi, deskripsi, dan setidaknya satu referensi publik, untuk kerentanan cybersecurity yang diketahui publik. CVE merupakan sebuah Sistem Common Vulnerabilities and Exposures (CVE) yang menyediakan metode referensi untuk kerentanan keamanan dan eksposur informasi yang diketahui atau dapat dikatakan CVE adalah sebuah katalog ancaman keamanan yang telah dikenali dan telah dilaporkan oleh seseorang, baik yang telah diperbaiki ataupun masih dalam proses perbaikan hole/celah tersebut. Menurut situs CVE, kerentanan adalah kesalahan dalam kode perangkat lunak yang memberikan penyerang akses langsung ke sistem atau jaringan.

Pada website CVE diberikan contoh data CVE yang dimana memiliki identitas **CVE-2017-12611**.



Vulnerability Details : CVE-2017-12611

In Apache Struts 2.0.1 through 2.3.33 and 2.5 through 2.5.10, using an unintentional expression in a Freemarker tag instead of string literals can lead to a RCE attack.

Publish Date : 2017-09-20 Last Update Date : 2017-09-29

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
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	Partial (There is reduced performance or interruptions in resource availability.)
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)	
CWE ID	20

Dari data diatas memiliki hole yang dimana Apache Struts 2.0.1 sampai 2.3.33 dan 2.5 sampai 2.5.10, menggunakan ekspresi yang tidak disengaja dalam tag Freemarker dan bukan string literal dapat menyebabkan serangan RCE. RCE adalah kemampuan penyerang untuk mengakses perangkat komputasi orang lain dan melakukan perubahan, tidak peduli di mana perangkat berada secara geografis. Remote Code Execution adalah dimana attacker melakukan injeksi coding melalui dengan mesin yang berbeda, maksudnya dilakukan secara remote terhadap mesin target.

Masalah dan solusi dari referensi data CVE **CVE-2017-12611**.

Problem

When using expression literals or forcing expression in Freemarker tags (see example below) and using request values can lead to RCE attack.

```
<@s.hidden name="redirectUri" value=redirectUri />
<@s.hidden name="redirectUri" value="${redirectUri}" />
<@s.hidden name="${redirectUri}"/>
```

In both cases a writable property is used in the `value` attribute and in both cases this is threatened as an expression by Freemarker. Please be aware that using Struts expression evaluation style is safe:

```
<@s.hidden name="redirectUri" value="%{redirectUri}" />
<@s.hidden name="%{redirectUri}"/>
```

Solution

Do not use such constructions in your code or use read-only properties to initialise the `value` attribute (property with getter only). You can upgrade to Apache Struts version 2.5.12 or 2.3.34 which contain more restricted Freemarker configuration but removing vulnerable constructions is preferable.

References Data CVE **CVE-2017-12611**.

– References For CVE-2017-12611

https://struts.apache.org/docs/s2-053.html CONFIRM

https://kb.netapp.com/support/s/article/ka51A000000CgttQAC/NTAP-20170911-0001 CONFIRM

http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-003.txt CONFIRM

http://www.oracle.com/technetwork/security-advisory/alert-cve-2017-9805-3889403.html CONFIRM

http://www.securityfocus.com/bid/100829
BID 100829 Apache Struts CVE-2017-12611 Remote Code Execution Vulnerability *Release Date:*2017-09-27