

Report Procedure:

**Vulnerability Name:**

Allocation of Resources Without Limits or Throttling

**CWE:**

CWE-770

**OSWAP:**

Allocation of Resources Without Limits or Throttling.

**Description:**

The HTTP/2 implementation accepted streams with excessive numbers of SETTINGS frames and also permitted clients to keep streams open without reading/writing request/response data. By keeping streams open for requests that utilised the Servlet API's blocking I/O, clients were able to cause server-side threads to block eventually leading to thread exhaustion and a DoS.

**Business Impact:**

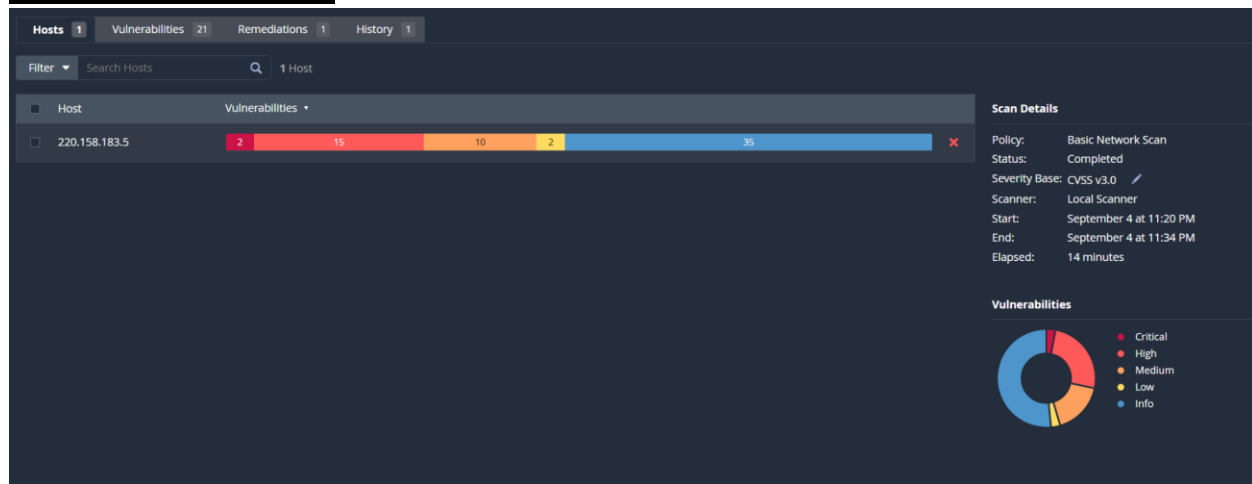
This is a type of attack that prevents the users from getting access to the system. This happens when the system the server of a website is overwhelmed with the amount of users this can lead to people not trusting the website and losing users due to lack of trust. This can also lead to interruption in the services that can cause more issues.

**Affected URL:**

URL: <https://vtop2.vitap.ac.in/vtop/initialProcess>

IPv4-220.158.183.5

**POC(Proof of concept):**




Sev	CVSS	VPR	Name	Family	Count		
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	28	🔄	✎
MIXED	...	...	TLS (Multiple Issues)	Service detection	4	🔄	✎
INFO	...	...	SSL (Multiple Issues)	General	6	🔄	✎
INFO	...	...	HTTP (Multiple Issues)	Web Servers	2	🔄	✎
INFO	...	...	IETF Md5 (Multiple Issues)	General	2	🔄	✎
INFO	...	...	TLS (Multiple Issues)	General	2	🔄	✎
INFO			Nessus SYN scanner	Port scanners	5	🔄	✎
INFO			Service Detection	Service detection	2	🔄	✎
INFO			Asset Attribute: Fully Qualified Domain Name (FQDN)	General	1	🔄	✎
INFO			Common Platform Enumeration (CPE)	General	1	🔄	✎
INFO			Device Type	General	1	🔄	✎
INFO			Host Fully Qualified Domain Name (FQDN) Resolution	General	1	🔄	✎
INFO			Inconsistent Hostname and IP Address	Settings	1	🔄	✎
INFO			Nessus Scan Information	Settings	1	🔄	✎

### Host Details

IP: 220.158.183.5  
DNS: 220.158.183.5.static-andharapradesh.powertel.in.183.158.220.in-addr.arpa  
OS: F5 BIG-IP Local Traffic Manager load balancer  
Start: September 4 at 11:20 PM  
End: September 4 at 11:34 PM  
Elapsed: 14 minutes  
KB: [Download](#)

### Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Sev	CVSS	VPR	Name	Family	Count			Scan Details	
<input type="checkbox"/>	CRITICAL	9.8	9.2	Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple ...	Web Servers	1	🔄	✎	<div>Policy: Basic Network Scan</div> <div>Status: Completed</div> <div>Severity Base: CVSS v3.0</div> <div>Scanner: Local Scanner</div> <div>Start: September 4 at 11:20 PM</div> <div>End: September 4 at 11:34 PM</div> <div>Elapsed: 14 minutes</div> <div><div>Vulnerabilities</div><div><div><div></div><div></div><div></div><div></div><div></div></div><div><div>Critical</div><div>High</div><div>Medium</div><div>Low</div><div>Info</div></div></div></div>
<input type="checkbox"/>	CRITICAL	9.8	6.7	Apache Tomcat 9.0.0 < 9.0.10 Multiple Vulnerabilities	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	8.6	5.5	Apache Tomcat 9.0.0.M1 < 9.0.21 vulnerability	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	8.1	9.2	Apache Tomcat 9.0.0.M1 < 9.0.1 Multiple Vulnerabilities	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	8.4	Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	6.7	Apache Tomcat 9.0.0.M1 < 9.0.16 DoS	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	6.7	Apache Tomcat 9.0.0.M1 < 9.0.20 DoS	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	6.7	Apache Tomcat 9.0.0.M1 < 9.0.30 Privilege Escalation Vulnerability	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	5.1	Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	5.1	Apache Tomcat 9.x < 9.0.40 Information Disclosure	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	4.4	Apache Tomcat 9.0.0.M1 < 9.0.68 Request Smuggling Vulnerability	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	4.4	Apache Tomcat 9.0.0.M1 < 9.0.10 multiple vulnerabilities	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	4.4	Apache Tomcat 9.0.0.M1 < 9.0.36 DoS	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	4.4	Apache Tomcat 9.0.0.M1 < 9.0.71	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	3.6	Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of S...	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.5	3.6	Apache Tomcat 9.0.0.M1 < 9.0.8 Denial of Service Vulnerability	Web Servers	1	🔄	✎	
<input type="checkbox"/>	HIGH	7.0	8.4	Apache Tomcat 9.0.0 < 9.0.35 Remote Code Execution	Web Servers	1	🔄	✎	

<input type="checkbox"/>	HIGH	7.5	4.4	Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability	Web Servers	1	🔄	✎
<input type="checkbox"/>	HIGH	7.5	4.4	Apache Tomcat 9.0.0.M1 < 9.0.10 multiple vulnerabilities	Web Servers	1	🔄	✎
<input type="checkbox"/>	HIGH	7.5	4.4	Apache Tomcat 9.0.0.M1 < 9.0.36 DoS	Web Servers	1	🔄	✎
<input type="checkbox"/>	HIGH	7.5	4.4	Apache Tomcat 9.0.0.M1 < 9.0.71	Web Servers	1	🔄	✎
<input type="checkbox"/>	HIGH	7.5	3.6	Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of S...	Web Servers	1	🔄	✎
<input type="checkbox"/>	HIGH	7.5	3.6	Apache Tomcat 9.0.0.M1 < 9.0.8 Denial of Service Vulnerability	Web Servers	1	🔄	✎
<input type="checkbox"/>	HIGH	7.0	8.4	Apache Tomcat 9.0.0 < 9.0.35 Remote Code Execution	Web Servers	1	🔄	✎
<input type="checkbox"/>	MEDIUM	6.5	4.4	Apache Tomcat 9.0.0.M1 < 9.0.5 Insecure C	Web Servers	1	🔄	✎
<input type="checkbox"/>	MEDIUM	6.5	4.2	Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10....	Web Servers	1	🔄	✎
<input type="checkbox"/>	MEDIUM	6.1	3.8	Apache Tomcat 9.0.0.M1 < 9.0.80	Web Servers	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.3	1.4	Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability	Web Servers	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.3		Apache Tomcat Default Files	Web Servers	1	🔄	✎
<input type="checkbox"/>	MEDIUM	4.3	2.2	Apache Tomcat 9.0.0.M1 < 9.0.12 Open Redirect Weakness	Web Servers	1	🔄	✎
<input type="checkbox"/>	MEDIUM	4.3	2.2	Apache Tomcat 9.0.0.M1 < 9.0.72	Web Servers	1	🔄	✎
<input type="checkbox"/>	MEDIUM	4.3	1.4	Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up	Web Servers	1	🔄	✎
<input type="checkbox"/>	LOW	3.7	2.2	Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitig...	Web Servers	1	🔄	✎
<input type="checkbox"/>	LOW	3.7	1.4	Apache Tomcat 9.0.0.M22 < 9.0.2 Insecure CGI Servlet Search Algorith...	Web Servers	1	🔄	✎
<input type="checkbox"/>	INFO			Apache Tomcat Detection	Web Servers	1	🔄	✎

## Vulnerabilities 21

**HIGH** Apache Tomcat 9.0.0.M1 < 9.0.36 DoS**Description**

The version of Tomcat installed on the remote host is prior to 9.0.36. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.36\_security-9 advisory.

- A specially crafted sequence of HTTP/2 requests could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive. (CVE-2020-11996)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

**Solution**

Upgrade to Apache Tomcat version 9.0.36 or later.

**See Also**

<http://www.nessus.org/u?e98498cd>

<http://www.nessus.org/u?45bd805e>

**Output**

```
Installed version : 9.0.0.M26
Fixed version    : 9.0.36
```

**CRITICAL** Apache Tomcat 9.0.0 < 9.0.10 Multiple Vulnerabilities**Description**

The version of Apache Tomcat installed on the remote host is 9.0.x prior to 9.0.10. It is, therefore, affected by multiple vulnerabilities.

A security misconfiguration vulnerability exists in Apache Tomcat prior to version 9.0.9 due to insecure default settings for the CORS filter (CVE-2018-8014).

A security misconfiguration vulnerability exists in Apache Tomcat prior to version 9.0.10. Hostname validation was not enabled by default when using TLS with the WebSocket client (CVE-2018-8034).

An information disclosure vulnerability exists in Apache Tomcat prior to version 9.0.10 due to a race condition. If an async request was completed by the application at the same time as the container triggered the async timeout, this could lead to a user being sent the response of another user (CVE-2018-8037).

**Solution**

Upgrade to Apache Tomcat version 9.0.9 or later.

**See Also**

<https://svn.apache.org/viewvc?view=rev&rev=1831726>

[https://tomcat.apache.org/security-9.html#Fixed\\_in\\_Apache\\_Tomcat\\_9.0.9](https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.9)

**Output**

```
Installed version : 9.0.0.M26
Fixed version    : 9.0.9
```

HIGH

Apache Tomcat 9.0.0.M1 < 9.0.30 Privilege Escalation Vulnerability

< >

**Description**

The version of Tomcat installed on the remote host is prior to 9.0.30. It is, therefore, affected by a privilege escalation vulnerability as referenced in the 'Fixed in Apache Tomcat 9.0.30' advisory.

- When using FORM authentication there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability. (CVE-2019-17563)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

**Solution**

Upgrade to Apache Tomcat version 9.0.30 or later.

**See Also**

<https://github.com/apache/tomcat/commit/1ecba14>  
<http://www.nessus.org/u7ba131b16>

**Output**

```
Installed version : 9.0.0.M26
Fixed version    : 9.0.30
```

Now from this report we get an idea of all the vulnerabilities that a website has. It tells us what are these vulnerabilities and also how critical they are. In this case, it tells us how safe the website is and what are the potential vulnerability threats that can happen on the website.

### Remediation:

Hosts	1	Vulnerabilities	21	Remediations	1	History	1
Search Actions <input type="text"/> 1 Action							
Action						Vulns	Hosts
Apache Tomcat 9.0.0.M1 < 9.0.80: Upgrade to Apache Tomcat version 9.0.80 or later.						26	1

To fix these vulnerabilities, we have to upgrade Apache Tomcat to any version 9.0.80 or later.