|  |  |
| --- | --- |
| From: | Christopher Gunn Kean Jin/KFHMB |
| To: | Muhammad Firdaus Khairuddin/KFHMB@KFHMB, Md Harmizam Md Aris/KFHMB@KFHMB |
| Date: | 16/03/2017 07:05 AM |
| Subject: | Fw: Global Threat Notification (16 March 2017) GTN # 000038 |

Team Security,

Please look into this one. Advise me accordingly please.

TQ

**Christopher Gunn**
Assistant Director
Information Technology

Tel: (+603) 2168 0000
Dir: (+603) 2168 0108
Email: christopher.gunn@kfh.com.my
[www.kfh.com.my](http://www.kfh.com.my/)
**@KFHMalaysia**

----- Forwarded by Christopher Gunn Kean Jin/KFHMB on 16/03/2017 07:04 AM -----

|  |  |
| --- | --- |
| From: | "Sysarmy Incident Response System" <cimc.sir@sysarmy.net> |
| To: | "GTN /GTI" <sysmy\_gtn@sysarmy.net> |
| Date: | 16/03/2017 12:50 AM |
| Subject: | Global Threat Notification (16 March 2017) GTN # 000038 |

-- reply above this line --

Dear Sir/ Madam,

CIMC Security Analyst team has created a ticket **GTN # 000038**.

A Global Threat Notification (New Remote Code Execution (RCE) Vulnerability in Apache Struts)
**Summary**

|  |  |  |
| --- | --- | --- |
| **Threat Notification**  | **:**  | New Remote Code Execution (RCE) Vulnerability in Apache Struts  |
| **Threat Type**  | **:**  | - Ransomware- DDOS  |
| **Outbreak Level**  | **:**  | Wild  |
| **Risk Level**  | **:**  | High  |
| **Attack Vector/Method**  | **:**  | - Web Access / OS Command Injection  |
| **Systems Affected**  | **:**  | Windows OS / Linux  |

**Details**The issue is a remote code execution vulnerability in the Jakarta Multipart parser of Apache Struts that could allow an attacker to execute malicious commands on the server when uploading files based on the parser. A vulnerability in the Struts 2 web application framework was patched and proof-of-concept exploit code was introduced into Metasploit (penetration testing software).

It allows a remote attacker to inject operating system commands into a web application through the “Content-Type” header. Written in Java, Apache Struts 2 is the popular open source web application framework. When an invalid value is placed in the Content-Type header, an exception is thrown. The exception is used to display the error to the user. An attacker can exploit this vulnerability to escape the data scope into the execution scope through the Content-Type header.

 **Indicator Of Compromised (IOC) :**
Attacker's IP:

-1.180.212.119
-103.20.126.36
-106.114.66.169
-110.240.226.100
-112.115.138.37
-113.139.88.198
-115.144.122.41
-117.104.136.243
-118.193.220.48
-120.33.90.142
-122.224.14.250
-124.116.254.225
-125.76.61.75
-146.20.3.205
-162.158.59.57
-173.70.39.121
-180.97.106.144
-182.245.212.189
-183.60.177.68
-192.241.130.69
-202.102.245.41
-211.148.31.6
-218.60.56.136
-221.218.83.75
-222.85.127.212
-23.212.108.44
-27.18.119.181
-36.5.182.128
-45.63.55.55
-52.220.191.24
-59.60.88.209
-61.188.38.140
-66.87.121.27
-73.83.105.250

User Agent:
- User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.0.3705

 **Impact :**
Web Server can be taken over by the attackers and use that to move laterally through your network. The attacker can use that to look for your domain controller and if the attacker find a way to compromise your password hashes, such as from the Linux server that have been compromised, they can possibly log in to your domain controller and use that to push malware to all machines. Ransomware could be sent by the attacker through the web server.
 **Vulnerability :**
- The flaw lives in the Jakarta Multipart parser upload function in Apache. It allows an attacker to easily make a maliciously crafted request (a malicious Content-Type value) to an Apache webserver and have it execute.
- The attacks are particularly risky to anyone running their Apache webservers as root. The risks are severe for an organization running an exposed Apache server if it’s compromised.

 **Recommendation :**
- Companies who use Apache Struts on their servers should upgrade the framework to versions 2.3.32 or 2.5.10.1 or switching to a different multipart parse implementation.

- Users who can not immediately upgrade to the patched Struts versions can apply a workaround that consists of creating a Servlet filter for Content-Type that would discard any requests not matching multipart/form-data. Web application firewall rules to block such requests are also available from various vendors.

 **Intelligence Sources :**
1) PCWorld website : http://www.pcworld.com/article/3178660/security/hackers-exploit-apache-struts-vulnerability-to-compromise-corporate-web-servers.html
2) Threat Post : https://threatpost.com/attacks-heating-up-against-apache-struts-2-vulnerability/124183/
3) Imperva website : https://www.imperva.com/blog/2017/03/cve-2017-5638-new-remote-code-execution-rce-vulnerability-in-apache-struts-2/