CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-070

MobileIron Critical Vulnerability

December 16, 2021 — v1.0

TLP:WHITE

History:

- *16/12/2021 — v1.0 – Initial publication*

Summary

On December 15th, Ivanti updated its advisory related to `CVE-2021-44228` vulnerability affecting MobileIron products [2]. While this CVE affects the Java logging library `log4j` [1], all products using this library are vulnerable to Unauthenticated Remote Code Execution.

Technical Details

The vulnerability exists in the Java logging library `log4j`. An unauthenticated remote attacker might exploit this vulnerability by sending specially crafted content to the application to execute malicious code on the server [1].

Affected products

- MobileIron Core
- MobileIron Sentry 9.13 and above
- MobileIron Core Connector
- MobileIron Core RDB

Recommendations

Ivanti provided guidance to mitigate the vulnerably on its various affected products:

1. Connect to the server CLI via SSH protocol;
2. Use the command `enable` to elevate privileges;
3. Install the workaround using one of the following commands (depending on the product you are updating):

```
install rpm url https://supportcdn.mobileiron.com/log4j-jndi/current/mi-workaround-log4j-jndi-
  vulnerability-1.0.0-1.noarch.rpm # MobileIron Core
install rpm url https://supportcdn.mobileiron.com/log4j-jndi/current/mi-workaround-sentry-
  log4j-jndi-vulnerability-1.0.0-1.noarch.rpm # MobileIron Sentry
install rpm url https://supportcdn.mobileiron.com/log4j-jndi/current/mi-workaround-connector-
  log4j-jndi-vulnerability-1.0.0-1.noarch.rpm # MobileIron Core Connector
```

```
install rpm url https://supportcdn.mobileiron.com/log4j-jndi/current/mi-workaround-rdb-
  log4j-jndi-vulnerability-1.0.0-1.noarch.rpm  # MobileIron Core RDB
```

4. Accept the service restart (`y`).

Notes:

- If FIPS mode is enabled on the server, then the effects of the installation will not persist across reboots. This means the RPM installation will need to be re-performed immediately after the system comes back up after a reboot.
- If the server is upgraded, then the RPM installation will need to be re-performed, unless the version being upgraded to has a fix to the issue.
- For Sentry, the RPM installation is applicable only to Sentry 9.13 and above. Versions prior to that are not vulnerable.

References

[1] https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-067.pdf

[2] https://forums.ivanti.com/s/article/Security-Bulletin-CVE-2021-44228-Remote-code-injection-in-Log4j