**TLP Amber**

# Advisory 2021-008: Active Exploitation of MobileIron products

The Australian Cyber Security Centre (ACSC) is aware of active exploitation of MobileIron products by malicious cyber actors, associated with the Log4j library vulnerability. Mitigations are available from Ivanti.

## Recommendations

Ivanti, the vendor, has identified configuration workarounds for impacted products and existing customers can access them here. They have advised that these mitigations are effective against CVE-2021-44228 and CVE-2021-45046. There is not currently a patch for either vulnerability. Organisations should contact Ivanti via support, follow the vendor on Twitter (@GoIvanti), and apply new patches as soon as they become available.

In addition to applying mitigations, organisations should investigate their complete MobileIron Core solution for evidence of compromise as a matter of priority (as previously detailed by the ACSC here).

## Details

The ACSC is aware of successful targeting and compromise of vulnerabilities associated with the Log4j logging library in a number of MobileIron products. Exploitation is evident across a wide variety of organisations. This has also been corroborated by other organisations globally (see here for more information).

Ivanti first released a temporary workaround on 12 December 2021. They subsequently added an RPM package on 13 December to enable persistence of the workaround through a server reboot.

The ACSC has liaised with Ivanti, and is aware that they are actively working on developing and releasing an effective patch. Ivanti has indicated that MobileIron Cloud is not vulnerable to CVE-2021-44228 and CVE-2021-45046.

## Assistance

The ACSC is monitoring the situation and is able to provide assistance and advice as required. Organisations that have been impacted or require assistance can contact the ACSC via 1300 CYBER1.

The ACSC has also published a technical Advisory on the Log4j vulnerability, which can be accessed at cyber.gov.au