

Motorola Solutions Technical Notification (MTN)

TITLE: CVE-2021-44228 and CVE-2021-45046 'Log4Shell' Java log4j Remote Code Execution vulnerability

TECHNOLOGY: ASTRO 25

SYMPTOMS:

KMF Server may be vulnerable to CVE-2021-44228 and CVE-2021-45046 'Log4Shell' Java log4j Remote Code Execution. Apache Log4j2 2.0- beta9 through 2.12.1 and 2.13.0 through 2.15.0 JNDI (Java Naming Directory Interface) features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP (Lightweight Directory Access Protocol), RMI (Remote Method Invocation), DNS (Domain Name System), HTTP (HyperText Transfer Protocol) or other JNDI (Java Naming Directory Interface) related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from the attacker controlled servers when message lookup substitution is enabled.

MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED:

KMF (Key Management Facility) box versions: R07.18.0442 and R10.00.0523 - R10.01.0050.

SEVERITY RECOMMENDATION:

Critical - Perform Workarounds and Corrective Actions

ROOT CAUSE:

Product is using Log4j libraries in versions 2.x - 2.15 that are impacted by this vulnerability.

DEFINITIVE TEST:

N/A

WORKAROUNDS AND CORRECTIVE ACTIONS:

As a general practice, we strongly recommend that our customers regularly take the following steps to reduce exposure and risk:

1. When possible, do not allow internet exposure for mission-critical devices and/or systems and, when internet exposure is required, always apply strong authentication controls including 2 factor authentication and VPN (Virtual Private Network) connection.
2. For security devices not provided by Motorola Solutions, contact your security device vendors (i.e., web application firewall vendors) to confirm that all detection or preventative capabilities have been applied.
3. For SUS (Security Update Service) and RSUS (Remote Security Update Service) customers, please ensure you have applied the latest updates, and McAfee Antivirus recent updates are deployed and working properly on all Microsoft Windows and Linux endpoints (servers, clients and workstations).
4. Review user and administrative accounts to ensure no unauthorized accounts are present. We are committed to protecting our customers and while we continue to conduct a robust investigation, we will keep our customers informed as further information becomes available.

ANY USE NOT APPROVED BY MOTOROLA SOLUTIONS IS PROHIBITED. This Motorola Technical Notification (MTN) is issued pursuant to Motorola's ongoing review of the quality, effectiveness, and performance of its products. The information provided in this bulletin is intended for use by trained, professional technicians only, who have the expertise to perform the service described in the MTN. Motorola disclaims any and all liability for product quality or performance if the recommendations in this MTN are not implemented, or not implemented in compliance with the instructions provided here. Implementation of these recommendations may be necessary for the product to remain compliant with applicable laws or regulations. Please be advised, that failure to implement these recommendations in the manner instructed may also invalidate applicable warranties, or otherwise impact any potential contractual rights or obligations. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2021 Motorola Solutions, Inc. All rights reserved.

RESOLUTIONS AND REPAIR PROCEDURES:

For non-redundant KMF configuration:

1. backup KMF database (coco kmf backup)
2. execute instructions from deployInstructions.txt file located on KC137V01I099990002.iso image

For redundant KMF configuration:

1. verify that Main KMF Server works in Active role (if not then perform switchover operation from Standby to Main)
2. backup database of Main KMF
3. on Standby KMF execute instructions from deplyInstructions.txt file located on KC137V01I099990002.iso image
4. on Main KMF execute instructions from deplyInstructions.txt file located on KC137V01I099990002.iso image
5. verify that Main KMF Server works in Active role (if not then perform switchover operation from Standby to Main)

Note: two switchover operations executed during the patching process will cause the KMF service to be not operational for up to 15 min.

To obtain the patching script:

- 1) Initiate a software request case through Motorola Solution, Inc. System Support Center (SSC) at 1-800-221-7144 (1-302-444-9800)
- 2) Await confirmation email from Motorola Solutions Software Factory with instructions
- 3) Complete the Motorola Solutions Software Factory Software Order Form:
 - a) Reference MTN-0026-22-NA in the 'Reason for Software/Hardware Change' section of the software order form.
 - b) Provide the part number **KC137V01I099990002** in the 'Part # or Version #' section of the software order form.
- 4) Email completed Software Order Form to MSSF for processing

In the event of disaster recovery, other KMF patch installation or KMF reinstallation this MTN needs to be reapplied.

PARTS REQUIRED (HARDWARE/SOFTWARE):

Patching script (applicable for all releases): KC137V01I099990002

ADDITIONAL INFORMATION:

It takes up to 15 minutes to patch KMFs working in redundant configuration. For non-redundant KMF, patching takes less than 8 minutes. OTAR Key Management functionality may not be available during patching.

REFERENCE THE FOLLOWING DOCUMENTS/PROCESSES FOR INSTALLATION PROCEDURES:

Please follow the specific product manual/documentation for update:

<https://learning.motorolasolutions.com/user-guide/66660enus>

Please see MTN-0279-21-NA document for instruction on patching other Astro system components.

WHEN TO APPLY RESOLUTION:

Immediately _X_

DOCUMENT NUMBER: MTN-0026-22-NA
APC: 137
ISSUE DATE: 01-2022
EXPIRATION DATE: 31-01-2023
Bulletin Type: Informational Only

LABOR ALLOWANCE:

This is an informational bulletin. No labor warranty is implied, intended or authorized for U.S. Domestic Partners/Customers. Other regions should follow their own standard procedures.

If, after attempting to perform the solution steps, you are having issues with the resolution in the MTN then please contact your MSI Technical support center.

https://www.motorolasolutions.com/en_us/support.html

SW ORDER FORM IS AVAILABLE UNDER THE LINK:

http://www.motorolasolutions.com/content/dam/msi/docs/robots/motorola-technical-notification/SW_order_form.pdf

ANY USE NOT APPROVED BY MOTOROLA SOLUTIONS IS PROHIBITED. This Motorola Technical Notification (MTN) is issued pursuant to Motorola's ongoing review of the quality, effectiveness, and performance of its products. The information provided in this bulletin is intended for use by trained, professional technicians only, who have the expertise to perform the service described in the MTN. Motorola disclaims any and all liability for product quality or performance if the recommendations in this MTN are not implemented, or not implemented in compliance with the instructions provided here. Implementation of these recommendations may be necessary for the product to remain compliant with applicable laws or regulations. Please be advised, that failure to implement these recommendations in the manner instructed may also invalidate applicable warranties, or otherwise impact any potential contractual rights or obligations. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2021 Motorola Solutions, Inc. All rights reserved.