ED-014-072

To: Edesix customers
Dec. 20, 2021

CVE 2021-44228 and CVE-2021-45046 Log4Shell Vulnerability

Motorola Solutions is aware of the Log4Shell vulnerability, CVEs-2021-44228 and CVE-2021-45046. The flaw is a remote code execution (RCE) vulnerability impacting the Java library Log4J for all versions 2.15 and earlier.

Based on our current analysis, the following Motorola Solutions products are not affected by the Log4J vulnerability:

- VB series body-worn cameras
- VT series body-worn cameras

We have determined that the following Motorola Solutions products may be impacted by the Log4J vulnerability:

- **VideoManager** - Our initial assessment indicates that the potential impact to VideoManager is **Low**. VideoManager is distributed as a number of components. Of those components, only the User Import Tool uses log4j. If you are not currently using the User Import Tool, then you are not affected by CVE-2021-44228. If you are using VideoManager's User Import Tool on your own servers (either with on-premises instances, or Motorola Solutions cloud services) then we believe you will not be affected by this CVE. All known exploits of it thus far would be ineffective and require elevated privileges in your environment to execute. It is prudent, however, to disable usage of the User Import Tool and wait for the next patch release of VideoManager.

  Next Steps

  ○ **Cloud Services:** If you subscribe to one of our cloud services and are using the built-in User Import Tool function, the user-import tool has been disabled on all cloud services to mitigate the risk presented by this CVE. For our cloud services, subject to existing customer-imposed change freezes, we will be upgrading your service to a patched release by **Monday 20th Dec.**, to re-enable the user-import-tool. This patch release will mitigate the risk presented by this CVE completely, and re-enables the user import tool (where used)

  ○ **On-Premises:** Motorola Solutions will issue a patch to the User Import Tool which will mitigate the risk presented by this CVE completely. This will be 15.1.7 for on-premises installations and is scheduled to be released by **Monday 20th Dec**.

We will continue to send additional updates to you directly as needed. Our analysis currently applies to Motorola Solutions software only.

As a general practice, we strongly recommend that our customers regularly take the following steps:

1. Ensure that your security monitoring or managed detection and response service has applied detection controls for exploitation of the Log4J vulnerability. The Cybersecurity & Infrastructure Security Agency (CISA) provides guidance on operational security controls here.
2. Contact your security device vendors (i.e., web application firewall vendors) to confirm that all detection or preventative capabilities have been applied.
3. Apply all updates provided by Motorola Solutions and other vendors, as soon as possible.
4. 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.
5. 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. Please direct questions to your local account management team.