Protecting Your Voice System Servers from Major Log4j Flaw - Updated Feb. 18, 2022

Gail Hovanec - 2022-02-19 - Product Notices & Alerts

UPDATE - FEB. 18, 2022

Honeywell has continued to release updated ECS for the impacted Voice software products as additional vulnerabilities were exposed. The current ECS releases update the log4j libraries to version 2.17.1, these further extend the fixes from log4j library version 2.15.0, 2.16.0, and 2.17.0.

Mountain Leverage Support can provide the Honeywell ECS appropriate for your system. Please email support@mountainleverage.com with your request.

UPDATE - DEC. 16, 2021

Regarding Mountain Leverage's mitigation strategy we advised this week, our developers completely removed the JndiLookup class from the .jar archive file which is the problem. This functionality is generally not used within the affected Honeywell Voice products, and our testing has confirmed that it can be removed without any negative impact. For stability reasons, we felt it was best to stay with the existing version of Log4j, but without the class file that can be exploited.

If your team would prefer to upgrade to a 2.16 file version, this is something that we can provide some assistance with, but we'll need to schedule this on a case by case basis.

Full details of the vulnerability can be found here.

ORIGINAL POST - DEC. 14, 2021

See Honeywell's statement here.

Over the last week, the IT and information security world has discovered a critical vulnerability within software commonly used on servers by companies of all sizes and industries around the globe. As you work to protect your data against these threats, Mountain Leverage is here to support you and your voice system by answering what we know so far:

What is the vulnerability?

The vulnerability lies within any Java-based web-server framework running *Apache Log4j*, an open-source Java package used to enable logging in many popular applications, and it can be exploited to enable attackers to gain full control of affected servers and launch ransomware attacks.

What servers does this affect?

Many servers and applications are affected. Systems and services that use the Java logging library, Apache Log4j, between versions 2.0 and 2.14.1 are all affected. In general, servers at risk of attacks include servers with open, external Internet access. However, if an attack enters your network by any means (including popular vulnerable applications such as Cisco, Google, Webex, etc.), it could enter other systems, including your Honeywell/Mountain Leverage voice system.

How does this affect my voice system?

Honeywell has confirmed the following voice system applications are at-risk:

VoiceConsole Version - Log4j Version

- 5.5 - Sept 2021 2.10.0
- 5.4 - June 2020 2.10.0
- 5.3 - Jan 2020 2.10.0
- 5.2.x - July 2019 2.10.0

VoiceLink Version - Log4j Version

- 5.1 - Jan 2020 2.12.1
- 5.0 - 2018 2.10.0

VoiceCheck Version - Log4j Version

- 1.8 - Jan 2021 2.7.0
- 1.7 - April 2019 2.6.2
- 1.6 - May 2018 2.6.0
- NOTE: The VoiceCheck transcription server is also affected and should be checked if used. This may be installed on a separate server for performance reasons.

The systems below are NOT affected by this exploit:

- VoiceConsole versions 5.1 or earlier
- VoiceDirect for ERP (VD-ERP) versions 2.1 and earlier
- VoiceLink 4.3 or earlier
- PickMaster
- OpsWare
- Orator

How do I mitigate this issue in my voice system?

Per recommendations from Apache, Mountain Leverage has provided modified libraries that do not contain the class with the exploit. We have tested this solution and can confirm it resolves the issue. Those files can be found here. This process should take about 15 minutes.

1. Search for any Log4j-core*.jar file on your server.
2. If the version is between 2.0 and 2.15, download the corresponding Log4j-core*-NO_JNDI.jar file from the link above.
3. Stop the VoiceLink, VoiceConsole, or VoiceCheck service.
4. Delete the existing Log4j-core*.jar file from your server. **The file must be deleted, otherwise your system is still vulnerable.**
5. Add the same Log4j-core*-NO_JNDI.jar file to the folder. Do not rename the file.
6. Start the VoiceLink, VoiceConsole, or VoiceCheck service.

For any questions or assistance in patching this exploit, please contact support@mountainleverage.com and we will be happy to help.

What else can I do right now?

Here are some additional resources that can help you mitigate the issue across your other servers:

- Apache Log4j Security Page
- Links to mitigation approach to many software packages

We are here for you around the clock and will keep you updated if further voice system mitigation needs are found as this situation evolves. You can revisit these instructions and see future updates on this page in our support portal. Please also ensure your IT organization is prioritizing this issue and investigating all of your vulnerable servers.

Mountain Leverage Support

866-984-9922, Ext.2

support@mountainleverage.com