Haivision Technical Bulletin

Distribution:	**Haivision Customers, Integrators, and Resellers**
Date:	2021-12-13
Subject:	Analysis of Log4J (CVE-2021-44228) Vulnerability in Haivision Products
Product(s):	All Haivision Products
Version:	All versions

This bulletin describes Haivision's analysis of the recent "Log4Shell" 0-day exploits of vulnerabilities in the Apache Log4J package.

Note: This version has been updated to include Haivision Play Pro and Haivision Play and Haivision Helper software as well as Furnace and CoolSign Server products.

Description

On 2021-12-09 security vulnerability in an open-source library called Apache Log4J was made public. For details, please see CVE-2021-44228 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 It has been subsequently reported by several security groups that there have been attackers launching exploits for this vulnerability for about two weeks. This vulnerability is commonly being referred to as "Log4Shell."

Haivision is glad to report that none of our shipping products (encoding/decoding appliances, server products, or cloud SaaS products) have been found to be at risk for compromise from this vulnerability.

Implications/Consequences

The Apache Log4J library is commonly incorporated into products by software developers to ease logging of events within the normal use of their software. Versions 2.14.1 and above are subject to this vulnerability. Log4J is mostly used in Java-based applications, but also may be included in products in other languages that depend upon other Java applications.
When successfully exploited, this vulnerability may allow remote code execution on vulnerable servers that allows attackers to insert tools to control the targeted systems.

Appliance products

- Makito Classic encoders/decoders: Not vulnerable. No dependence upon Log4J.
- Makito X encoders/decoders: Not vulnerable. No dependence upon Log4J.
- Makito X4 encoders/decoders: Not vulnerable. No dependence upon Log4J.

- **Haivision Play Set-Top-Boxes** (Play 1000, Play 2000, Play 4000): Not vulnerable. No dependencies upon Log4J in Haivision software or in vendor firmware.

Server Products

- **Haivision Media Platform**: Not vulnerable. No dependence upon Log4J.
- **Haivision Media Gateway**: Not vulnerable. No dependence upon Log4J.
- **Haivision SRT Gateway**: Not vulnerable. No dependence upon Log4J.
- **Haivision Kraken**: Not vulnerable. No dependence upon Log4J.
- **Haivision KB encoders**: Not vulnerable. No dependence upon Log4J.
- **Haivision Connect DVR**: Not vulnerable. No dependence upon Log4J.
- **Haivision Furnace (EOL: 2022-01-15)**: Not vulnerable. No dependence upon Log4J.
- **Haivision CoolSign (EOL: 2022-01-15)**: Not vulnerable. No dependence upon Log4J.

Cloud SaaS Solutions

- **Haivision Hub**: Not vulnerable. Hub does utilize a package that is built with Log4J, but the version used is not vulnerable and the specific configuration implemented would prevent exploitation.
- **Connect**: Not vulnerable. Connect does utilize a package that is built with Log4J, but the version used is not vulnerable and the specific configuration implemented would prevent exploitation.
- **Haivision Video Cloud**: Not vulnerable. No dependence upon Log4J.
- **Lightflow**: Not exploitable. Lightflow does utilize a package built with a vulnerable version of Log4J, but the specific configuration implemented prevents remote execution.
- **Haivision P2P**: Not exploitable. Haivision P2P does utilize a package built with a vulnerable version of Log4J, but the specific configuration implemented prevents remote execution.

Software Applications

- **Haivision Play Pro** (IOS, Android): Not vulnerable. No dependencies upon Log4J.
- **Haivision Play Mobile** (IOS, Android): Not vulnerable. No dependencies upon Log4J.
- **Haivision Helper** (Windows, Mac OSX): Not vulnerable. No dependencies upon Log4J.

Recommended Course of Action

No action is required for deployed appliance and server products.

On 2021-12-10, the Haivision cloud product development teams confirmed that no immediate risk of exploitation existed for the listed SaaS solutions. However, we are prioritizing the patching of vulnerable services and will be deploying fixes in the coming days.

Next Steps

There is no action required from our customers at this time. We greatly value the trust our customers place in Haivision, our products and services, and will continually work to earn and validate that trust.

If you would like further technical advice on this vulnerability and Haivision's response, please contact Haivision Technical Support.

References

CVE-2021-44228
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

Haivision Product End of Life Policy
https://support.haivision.com/s/article/Product-End-of-Life-Policy

Contact Information

Haivision Technical Support
2600 Blvd. Alfred-Nobel
5th Floor
Montreal (Quebec) Canada H4S 0A9
+1.514.334.5445
tickets@haivision.com

Haivision continues to monitor this and other security issues and will provide updates to our customers as they become available.

The Haivision Technical Support Team