21 December 2021

AND PHONE APPLICATION SERVER – VULNERABILITY STATEMENT - CVE-2021-45105

A vulnerability was discovered in the Apache log4j logging component published on 10 December 2021. Several incremental updates were published in the following days, as Apache worked to resolve the issue. This statement references the latest vulnerability, CVE-2021-45105. The Product and R&D team has reviewed the product in relation to the latest update. Where the Log4j component is used, this document provides recommendations and / or mitigating action.

Enghouse will continue to monitor the status and advise on any recommended action.

Description

The vulnerability impacts Apache-Log4j 2 versions 2.0 through to 2.16. The issue has been resolved by Apache in version Log4j version 2.17 and 2.12.3. Links to further information is provided in the following table.

Update	More information
Current, as of 20 Dec 2021	https://nvd.nist.gov/vuln/detail/CVE-2021-45105
Related	https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Risks and Exposure

Andtek uses Java and log4j as logging tool which means that Andtek is affected by this vulnerability.

Recommendations and required actions

To mitigate the problem, please execute the following steps:

1. Immediate counter measures: switch to a very low log level such as FATAL or ERROR. No soft-restart required. This will reduce likelihood of exploitation.

2. APAS 6.x: apply "APAS 6.x Log4j Vulnerability Hotfix" from service.andtek.com.