20 December 2021

ENGHOUSE COMMUNICATIONS CENTER – 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

Our analysis has shown that Communications Center is affected, but only for those installations using Nuance for IVR or Communications Portal.

Nuance Issued a statement where it acknowledges that Nuance Speech Suite 11.x is the most affected by this vulnerability.

- Nuance will be posting a web page soon with details on what's impacted and the plan to mitigate.
- The necessary fix to Nuance Speech Suite 11.x will require upgrading to version 11.0.9 along with a forthcoming patch.
- Nuance still doesn't have an ETA on the required patch.

Problem mitigation

No action is required for Communications Center (CC). For the integrated business applications, potential vulnerabilities should be mitigated as specified by the respective vendors

Recommendations and required actions

Below are the recommendations for the core product and any included third-party components:-

PRODUCT or COMPONENT NAME & VERSION	Impact	Recommendation	Required action
Communications Center 9.x - current	No impact. If Nuance used, unknown.	If Nuance used, wait for mitigation recommendations and update on a patch from Nuance.	If Nuance used, analysis underway. No action required, at this moment but mitigation actions will be shared soon. Permanent fix for Nuance Speech Suite 11.0.x we'll require upgrade to Nuance Speech Suite 11.0.9 and patch to be released.