NATILIK

London | New York | Sydney

Natilik response to Log4j vulnerability

Published: 17th December 2021

Natilik has implemented procedures to scan our environment for vulnerabilities. Any such vulnerabilities identified will be monitored and tracked until remediated. In addition, regular vulnerability assessments are run to determine whether key controls are operating effectively. Any findings are categorised by risk level and modifications to the environment are implemented accordingly.

The Natilik IT team regularly monitors external security vulnerability awareness sites, and as part of the routine vulnerability management process, the Natilik IT team will evaluate the exposure to these vulnerabilities and will act to mitigate risks when necessary.

Specific to Log4j, Natilik is actively monitoring vulnerabilities across all products and services. The first [1] issue was reported on Friday, 10 December 2021. A second related issue [2] was reported Tuesday, 14 December 2021.

Our security teams have been analysing our products and services to identify and mitigate any instances of CVE-2021-4428 and CVE-2021-45046 in Apache Log4j. Currently, Natilik is not aware of any impact to the security of our external enterprise systems & services and have remediated several internal systems that were found to be affected. The remaining systems, which are pending the release of a fix from the relevant vendor, have been assessed and where appropriate access to those systems has been further restructured to mitigate the chance of exploitation.

If you have any questions or concerns about this matter, please contact support@natilik.com, your account or service delivery manager.

Security and reliability continue to be top priorities for Natilik as they are priorities for our partners and clients, we will continue to monitor the situation and will publish further updates should the situation change.

Mark Dibella
Chief Information Officer

[1] The Log4j vulnerability (CVE-2021-44228) permits unauthenticated remote code execution (RCE) on any Java applications running a vulnerable version of Apache's Log4j 2. It poses a severe risk to those using this version, because it can permit unauthorized access or complete control over systems when exploited correctly.

[2] The Log4j limited mitigation issue (CVE-2021-45046) invalidates previous mitigations in some cases. These vulnerabilities are fixed in Log4j 2.16.0.

9A Devonshire Square, London EC2M 4YN

T +44 203 597 8000 | E hello@natilik.com

natilik.com

Natilik Limited
Registered in England & Wales Number: 595 4905 | VAT 894 3202 16