Letter of Attestation – Sophos: UTM

Summary

This letter confirms that Nettitude, an award-winning provider of cybersecurity services, has carried out a security assessment on behalf of Sophos, over June and July 2022.

Assessment Scope

The assessment was carried out against Sophos' UTM product. The following product components were assessed:

- UTM: Web Application/Thick Client
- UTM: Code-assisted Web Application/Thick Client

There were no significant exclusions.

Assessment Methodology

The assessment was carried out using Nettitude's Gey Box and White Box testing methodology.

A Grey Box test is a blend of Black Box testing techniques and & White Box testing techniques. In Grey Box testing, clients provide Nettitude with snippets of information (such as source code in this case) to help with the testing procedures. This results in a highly focused test.

Assessment Details

The product assessment was carried out between the dates 20th June 2022 and 18th July 2022. The assessment comprised of a total of 20 person days of effort.

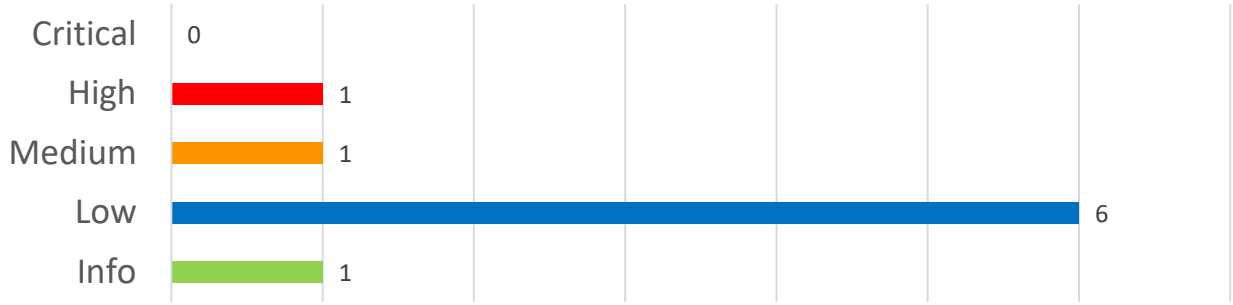
www.nettitude.com

T: +44 0345 5200 085
info@nettitude.com

1 Jephson Court , Tancred Close, Leamington Spa,
CV31 3RZ, United Kingdom

Findings summary

The assessment identified nine findings. The following table explains the severity of those findings.



About Us

Nettitude is an award-winning provider of cybersecurity services, bringing innovative thought leadership to the ever-evolving cybersecurity marketplace. Leveraging our tenacious curiosity, we aim to operate at the forefront of the industry. Through our research and innovation centres, Nettitude provides threat led services that span technical assurance, consulting and managed detection and response offerings.

Qualification

This letter serves to outline the type and duration of testing carried out. Nettitude carries out all testing in line with industry best-practise, but testing is time-limited and contingent on the level of information provided and the versions of software tested. This letter does not guarantee that:

- The product(s) do not have any further vulnerabilities, or that modifications to the product, its dependencies or the ways in which it is used will be safe from new security vulnerabilities.
- The product is compliant with any regulatory requirements (unless noted above)
- Vulnerabilities identified have been remediated in the product