DOCUMENT VERSION 2.0 – 01/02/2020

Cyber Hygiene Vulnerability False Positive Assertion

CISA's Cyber Hygiene team defines a false positive as data that incorrectly indicates a specific vulnerability is present on a customer's public facing network. After receipt of this form, CISA will quickly review that all fields have been adequately completed and will subsequently mark the finding as a false positive. Findings marked as false positives will stop appearing in the main body of the report for one year and, instead, will be reported in a separate appendix along with their respective false positive effective and expiration dates.

CISA reserves the right to assert that certain findings are not false positives (e.g. risk acceptance), and when false positive assertions are accepted by CISA, that acceptance should not be construed as validation that a finding is in fact a false positive. CISA will periodically conduct false positive reviews. This will not include exploiting a vulnerability but may include actively communicating with the host in question. If our research appears to confirm your analysis, the false positive marking will remain in effect until its original expiration date; however, if the analysis can reasonably prove the risk still exists, CISA will engage in discussions with your organization before removing any false positive markings.

Please complete all of the following:

1) The date of the most recent report that has the false positive: MM/DD/YYYY _____

2) The severity & full name of the vulnerability: Ex: Critical, PHP Unsupported Version Detection _____

3) The affected host(s) & respective port(s):

Example: 8.8.8.8:80,443 8.8.8.9:443

4) If attaching false positive evidence (e.g. screen shots of configuration files showing patch), provide a summary below for each on why it is included. Please specify where to look if not immediately evident (such as long email chains). Do not include screen shots of your Cyber Hygiene report.

Example: 1) "Attachment 1" screenshot configuration file showing updated PHP version. 2) See email conversation dated MM/DD/YYY between Bob and Alice about updating version.

5) Provide as detailed an explanation as possible as to why the vulnerability is a false positive, referring to specific attachments where appropriate. Specify if false positive assertion is due to implementation of compensating controls to mitigate the detected vulnerability.

Example: Banner will still show unsupported PHP but evidence provided proves we have updated the version.

Please send this completed form and any attachments through your designated technical point of contact to NCATS@hq.dhs.gov. CISA recommends zipping & encrypting the submission package.