DOCUMENT VERSION 1.2 – 03/18/2019

# Cyber Hygiene Vulnerability False Positive Assertion

NCATS Cyber Hygiene team defines a false positive to be data that incorrectly indicates a specific vulnerability is present on a customer's public facing network. After receipt of this form, NCATS will review and perform our own analysis which will not include exploiting a vulnerability, but may include actively sending packets to the host in question.

If our research appears to confirm your analysis, the vulnerability will be marked as a false positive for that host and port and will stop appearing in the main body of report for one year. Vulnerabilities marked as 'false positive' will be reported in a separate appendix along with the dates the false positive took effect and when it will expire.

NCATS reserves the right to assert that certain findings are not false positives (i.e. risk acceptance), and when false positive assertions are accepted by NCATS, that acceptance should not be construed as validation that a finding is in fact a false positive.

**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 (ex: screen shots of configuration files showing patch) in submission, provide a summary below for each on why it is included. Please specify where to look if not immediately evident (such as long email trains). 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. NCATS recommends zipping & encrypting the submission package.**