From: [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] FW: My feedback on 171r3 is not published
Date: Friday, July 28, 2023 1:28:28 PM
Attachments: [redacted]

Resending.

From: Kenneth Benjamin [redacted]
Date: Friday, July 28, 2023 at 7:56 AM
To: Pillitteri, Victoria Yan (Fed) [redacted], Ross, Ronald S. (Fed) [redacted]
Subject: My feedback on 171r3 is not published

Hi,

I sent the feedback below but don't see it in the public comments list. Can you please ensure that it's included in your deliberations?

Thanks,
Ken

Kenneth Benjamin, CEO
Island Systems, LLC
[redacted]
Get on my calendar: [redacted]
https://islandsystems.net

From: Kenneth Benjamin
Sent: Friday, July 14, 2023 9:30 AM
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>
Subject: 3.14.1(b) feedback

3.14.1. Flaw Remediation:

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

c. Install security-relevant software and firmware updates within [Assignment: organization defined time period] of the release of the updates.

Whereas 3.14.1(c) provides protection for the confidentiality of CUI, 3.14.1(b) is primarily about availability, and should be tailored out.

For example, we market a virtual desktop solution in which we rely on automated patching, e.g., Windows Update, from reliable vendors, the selection of which is covered by section 3.17. By policy, we define the 3.14.1(c) ODP as 7 days. We also specify that the confidentiality benefits of applying vendor updates is greater than the risk to availability that might arise from a defective update. This is particularly important due to the prevalence of zero-day vulnerabilities which could lead to a loss of confidentiality.

In practice, the vast majority of 3rd party non-security-related flaws have no impact on the system and do not require testing. Most are product feature improvements, functional bug fixes that impact specific users, or only apply to specific configurations, which most users don't have. Gross defects are relatively rare in commonly used software.

The way this currently reads, it would appear that organizations will be required to perform tests on all software and firmware (SW) updates before deploying them, to include all 3rd party supplied SW. Organizations are not qualified to, and do not have adequate resources or access to the source code needed to perform anything more than functional tests in their environment, which I believe is the intent of the control, but not the language.

In addition, the purpose of the testing is not clear. "Effectiveness and potential side effects" could mean that the update resolves an issue related to integrity and availability, for which an organization may be able to perform functional tests, or it could include security impacts, which are not going to be well understood by organizations, regardless.

For most organizations, and particularly SMBs, they don't have the ability to perform testing beyond basic functional testing during repair of system operational defects, usually related to a misconfiguration. They have no ability to test 3rd party SW, and certainly not better than the SW manufacturer. Furthermore, testing updates before deployment is impractical in smaller organizations, and offers little value to the confidentiality of the system for the reasons already stated.

I recommend the following options for 3.14.1(b) (in order of preference):

1. Remove from 800-171r3 (strongly preferred option)
2. Apply only to 1st party defects within the system, e.g., organization developed software, availability / integrity failure remediation such as configuration defects
3. Allow for an ODP to specify the scope, timing, and responsibility for testing, e.g., "vendors shall be responsible for testing SW prior to release"
4. Require the use of software/firmware vendors that perform tests (should be in 3.17 or

possibly bring in something from SA, not 3.14)

Thanks,

Kenneth Benjamin, CEO
Island Systems, LLC
[redacted]
Get on my calendar: [redacted]
https://islandsystems.net