Executive Order – NIST workshop position paper #1

(Criteria for designating "critical software")

Microsoft Corporation

Focus Area

Criteria for designating "critical software." Functional criteria should include, but not be limited to, level of privilege or access required to function, integration, dependencies, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised. See EO Section 4(g).

Microsoft Response

Determining what information, systems, and assets are most critical, sensitive, or high value is a foundational risk management activity that enables organizations to invest security and resiliency resources in a manner that aligns with risk priorities. Designating "critical software" should be part of this broader exercise, supporting continuity in organizational strategies to assess and manage technology-based assets and potential impacts of greatest concern.

There is variability in the function and risk profile of different software products and usage scenarios, and criteria for designating critical software should reflect these distinctions. Within the May 12 *Executive Order on Improving the Nation's Cybersecurity*, there is a recognition of function-based criteria appropriate for defining critical software, including level of privilege or access required to function, direct access to networking and computing resources, and performance of a function critical to trust. There is also recognition of criteria related to a risk profile, including potential for harm if compromised.

Beyond the criteria introduced above, Microsoft proposes that a framework for defining and designating critical software includes additional criteria related to risk profile. Such criteria should include characteristics of usage and the context of usage scenarios as well as ways to further define the potential for harm if compromised. Existing U.S. Government definitions of a "high value asset" offer criteria for consideration, including by recognizing the importance of "critical programs that are of particular interest to…adversaries" and by establishing that assets, systems, information, and data are "high value" when unauthorized access, modification or disruption could have a significant impact on U.S. national security interests, foreign relations, the economy, or public safety.[1]

Leveraging such criteria serves to narrow the scope of critical software to those software products, usage scenarios, and operational contexts that present the greatest risk. Alternatively, an overly broad approach to designating critical software risks applying criticality labels too widely, undermining the significance of the designation and stretching agency focus and risk management resources beyond those scenarios or contexts of greatest concern.

However, beyond starting with a framework of functions-based and usage criteria, there is a complex set of trade-offs to consider in taking a centralized or more distributed approach to designating critical software. We're encouraged by the potential for a federated model of establishing criteria and consistently applying such criteria to federal agency operations in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), balancing interests in focusing resources on agency risk

[1] High Value Asset - Glossary | CSRC (nist.gov)

priorities with the need to strengthen clarity for technology providers and operators as well as centralized U.S. Government risk management functions.

We also encourage the U.S. Government to take an iterative, phased approach. An initial phase of designations should focus on software functions, usage scenarios, and operating contexts of greatest concern, enabling agencies to apply criteria fully, establish confidence in their initial inventories of critical software, and implement security measures in a prioritized manner. This narrowly focused exercise will also prepare agencies to undertake additional phases of analysis and security measures implementation with appropriate processes and resources in place to do so effectively.

Recommendations

1. Leverage a framework for defining and designating critical software. The framework should contain at least three types of criteria: 1) functions-based or -related criteria, which capture for what software is used and what implications result (e.g., direct access to networking and computing resources, level of privilege or access required to function); 2) characteristics of usage (e.g., integration and dependencies with other software, amount of usage and resulting "blast radius" of incidents); and 3) context of usage, including threat profile, user profile, and potential impacts of unauthorized access, modification, or disruption. Ultimately, these criteria help agencies consider the value of assets or data relying on software products. This approach also captures that, if critical software is exploited, there are significantly harmful impacts, including access to highly sensitive data and/or disruption of the continuity of a high value system, service, or infrastructure.

2. Key questions to consider for designating critical software:
    a. Who is interacting with software (e.g., a privileged user like an administrator; a high priority user with high impact availability demands)?
    b. For what purpose is software being used (e.g., for a function that's critical to national security or economic resiliency), and what would be the impact of a disruption?
    c. To what extent is software being used across an environment, impacting recoverability in the context of incident response (e.g., broadly across agencies or for a narrow subset of a single agency's data, systems, or services)?
    d. To what data does software have access (e.g., to highly sensitive or confidential data)?

Request to participate on panel

Microsoft would welcome the opportunity to participate on the panel that will lead the discussion regarding criteria for designating "critical software" at the June 2 – 3, 2021 NIST workshop. For this discussion, we will share content on our approach to developing criteria for and defining critical or high value systems and assets.