The Software Alliance

BSA

# Focusing on Exploited Vulnerabilities

## An Opportunity to Improve Cybersecurity

In today's connected world, cybersecurity has become a critical concern for individuals, businesses, and governments alike. Malicious actors are constantly searching for vulnerabilities to exploit while enterprise technology companies and their customers are constantly working to make the most of their cybersecurity investments.

### Differentiating Vulnerabilities

As the US National Cybersecurity Strategy recognizes, "even the most advanced software security programs cannot prevent all vulnerabilities." But not all vulnerabilities are created equally.

Some vulnerabilities, because of how the software is designed and deployed, cannot be exploited. Other vulnerabilities are known to be exploited by malicious actors and need to be prioritized. The US government maintains a specific database for such exploited vulnerabilities, the Known Exploited Vulnerabilities (KEVs) Catalog.

### Addressing Vulnerabilities

Software producers and their customers can address a vulnerability, including an exploited vulnerability, in multiple ways.

One way to address a vulnerability is patching. Developing and deploying a patch can be complicated. Any given piece of software might depend on an external software library or another piece of software. And if the vulnerability is in the underlying software library, the software producer might depend on a third-party to patch a vulnerability in that library before the software producer can develop its own a patch. Additionally, in some cases, once a software producer has developed a patch, it may have to rely on customers updating their software.

A second way to address a vulnerability is deploying a compensating control (i.e., a management, operational, or technical countermeasure targeted to mitigate a vulnerability). A compensating control can reduce the risk posed by the vulnerability to an acceptable level or nearly eliminate the risk altogether.

### Improving Software Security and the Security of the Digital Ecosystem

When and how to address a vulnerability should be a risk-based decision. Arbitrary deadlines for developing and deploying patches are not the most effective approach to improve cybersecurity. For example, a requirement that specifies a period to patch a vulnerability that is *not* exploitable as deployed will not produce the best security outcomes.

Software producers and their customers should prioritize addressing exploited vulnerabilities over vulnerabilities that are either not exploitable as deployed or not known exploited vulnerabilities. Similarly, software producers and their customers should take a risk-based approach to decisions about patching or deploying compensating controls, and, to the extent possible, use artificial intelligence (AI) and automation to reduce the time to discover and respond to vulnerabilities. A risk-based approach will help resources flow to the challenges that pose the highest risk.

Software producers continue to improve their development practices and produce software with fewer vulnerabilities. However, when a software producer discovers a vulnerability, it should take a risk-based approach to addressing it, prioritize known exploited vulnerabilities, and automate discovery and remediation, when possible, which will ensure it leverages its cybersecurity resources to their greatest effect.