

CVE Program Reserved but Public (RBP) Policy

Document Version: 2.0.0

CVE Board Approval: August 13, 2026

Purpose

[CVE Numbering Authorities \(CNAs\)](#) support the CVE Program by reserving and assigning [CVE IDs](#), creating [CVE Records](#), and publishing them to the [CVE List](#). Prompt publication ensures consistent, timely vulnerability information is available for defenders to take action. The CVE Program “Reserved but Public (RBP) Policy” defines how the CVE Program monitors and enforces timely CVE Record publication after Public Disclosure of a CVE ID.

The RBP Policy is designed to maintain flexibility while providing clear guidelines for the [Secretariat](#), [Top-Level Roots](#) (TL-Roots), and [Roots](#) to consistently measure, assess, and determine the best course of action in resolving RBPs under a defined, practical framework.

Scope

The CVE Program RBP Policy applies to all CVE Program CNAs.

Background

A [Reserved but Public](#) (RBP) CVE ID is defined as:

- A CVE ID in the “Reserved” state that is referenced in one or more public sources but for which a CVE Record has not been published.

Timely Publication

A CVE Record should be published within 72 hours of either (a) disclosure by the CNA or (b) the CNA becoming aware of a third-party disclosure, as applicable. CNAs should ensure timely publication of CVE Records, recognizing that such publication may, at times, coincide with ongoing vulnerability or incident response activities. Vulnerability exploitation can begin shortly after Public Disclosure, often within hours.

CNAs MUST prioritize requests from their TL-Root or Root to publish CVE Records for RBPs identified as critical.

The CVE Program does not condone any unnecessary, intentional, or routine delay between Public Disclosure of vulnerability information (e.g., advisory or Fix) and CVE Record publication.

The CVE Program recognizes that internal processes may necessitate short delays; however, time flexibility allowed by the CNA Operational Rules should not be used to intentionally delay publication once an advisory or Fix has been made public. A delay intended to limit the

discoverability of public vulnerability information is inconsistent with CVE Program expectations and often benefits attackers more than defenders

CNA Operational Rules Alignment

CNA Public Disclosure (Requirement)

- **CNA Rule 4.5.1.4:** CNAs MUST publish a CVE Record to the CVE List within 72 hours of Publicly Disclosing a CVE ID assigned by the CNA. If the CNA does not publish within 72 hours, then the CNA's [Root](#) MAY direct the appropriate [CNA-LR](#) to publish a CVE Record for the assigned CVE ID. Ownership of the CVE Record MAY be transferred.

Third-Party Public Disclosure (Strong Expectation)

- **CNA Rule 4.5.1.6:** CNAs SHOULD publish CVE Records within 72 hours of becoming aware that a CVE ID assigned by the CNA has been Publicly Disclosed by a party other than the CNA.

RBP Tracking

RBPs may be identified by CVE Program TL-Roots, Roots, and the Secretariat via:

- Monitoring public sources for disclosed CVE IDs
- Reports from vendors, researchers, CNAs, or the public
- Program metrics and audits
- Direct communication with CNAs

Notification and Remediation

When an RBP is identified that is in violation of Program Rules 4.5.1.4 or 4.5.1.6 exceeding the 72 hours:

1. The TL-Root or Root will notify the CNA of affected CVE ID(s) and the required remediation timeline (as defined by the TL-Root and/or Root).
 - a. A CNA may be deemed unresponsive (refer to the CVE Program Policy for Inactive CNAs if the CNA does not acknowledge or respond within the timeframe specified in the notice (or, if unspecified, within a reasonable operational timeframe consistent with Program practice)).
2. The CNA is expected to publish RBPs as soon as possible and no later than the deadline stated by their TL-Root or Root (which may account for factors such as volume, complexity, and resource constraints).
3. 3. If the CNA still doesn't act, the Root or TL-Root can delegate publication to a CNA-LR (reference [CNA Rule 4.5.1.4](#)).

Enforcement

The CVE Program may take further action depending on the CNA's volume, history, and severity of RBPs. The table below highlights potential corrective actions they may be applied individually or combined:

Action Level	Requirements & Impact
Warning	CNA must provide a formal plan of action
Reservation Caps	Quota reductions or temporary suspension of new CVE ID reservations.
Intervention	A Root may direct a CNA-LR to publish or transfer record ownership.
Formal Review	Formal program review; may lead to new conditions of participation.

Any CVE ID reservation restrictions are lifted once the CNA has published all outstanding RBPs or resolved the matter to the satisfaction of the TL-Root, Root, or Secretariat. Repeated violations of the RBP policy may result in additional sanctions, up to and including CNA decertification.