Status: **DRAFT**
Shared with: NetSec Committee
Reviews: Subgroup → NetSec → CA/B Forum

SC39 Ballot: Critical Vulnerability Definition

Motivation & Background

It was brought to the attention of the NetSec Subgroup that the URL which points to the definitions of the CVSS security scoring system is no longer the appropriate one; moreover the definition of “Critical Vulnerability” is no longer strictly correct by the definitions currently posted by NIST.

Considerations

Definitions of terms should always be consistent, especially when the term is canonically defined by an external body; references should be updated as and when they change on the canonical source.

Risk Analysis/Benefits

Using definitions which are no longer supported is a risk in itself. Since there are normative statements around the handling of Critical Vulnerabilities we consider that having a current and actively supported definition reduces risk.

It is true that the definition of Critical Vulnerability reduces the scope of such vulnerabilities (from CVSS v2.0 score of 7.0+ to CVSS v3.0 score of 9.0 and above) but this reflects the finer grained detail which triggers urgent emergency action on behalf of those consumers of the NVD reports. We do not consider that the move to a more detailed scale represents an substantive increase in risk to CAs and those who place trust in them.

In terms of a (crude) quantitative analysis, looking at the CVSSv3 scores for 2020 [13206 items overall] which are >= 9.0 (ie, Critical) but which have a CVSSv2 score of <= 7.0 (ie, below Critical under the older definition which are actually considered Critical under the new), we see there are 252 such disclosed vulnerabilities, or 1.9% [sourced from nvd.nist.gov]; conversely we find that there are 274 vulnerabilities which have a CVSSv2 score of >= 7.0 but which have a CVSSv3 score of <= 9.0, or 2.07% (that is, that would be Critical under the old definition, but not under the new one). Thus there is a very slight increase (0.17%) in vulnerabilities which would be

considered Critical under the status quo, but not under the proposed ballot definition. This is balanced against the finer detail which goes into consideration of CVSSv3.x scoring.

Ballot

The following motion has been proposed by Neil Dunbar of TrustCor and endorsed by Ben Wilson (Mozilla) and Corey Bonnel (DigiCert).

--- MOTION BEGINS ---

This ballot modifies the “Network and Certificate System Security Requirements” based on Version 1.5.

Under the section “Definitions”:

Remove the current definition:

> **Critical Vulnerability**: A system vulnerability that has a CVSS score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see http://nvd.nist.gov/home.cfm), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.

Insert a new definition:

> **Critical Vulnerability**: A system vulnerability that has a CVSS v3.0 score of 9.0 or higher according to the NVD or an equivalent to such CVSS rating (see https://nvd.nist.gov/vuln-metrics/cvss), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.

--- MOTION ENDS ---

*** WARNING ***: USE AT YOUR OWN RISK. THE REDLINE BELOW IS NOT THE OFFICIAL VERSION OF THE CHANGES (CABF Bylaws, Section 2.4(a)):

A comparison of the changes can be found at:

https://github.com/cabforum/documents/compare/8f63128...neildunbar:54c201f?diff=split

This ballot proposes one Final Maintenance Guideline.

The procedure for approval of this ballot is as follows:

Discussion (7+ days)

Start Time: <INSERT>

End Time: <INSERT>

Vote for approval (7 days)

Appendix: CVE Vulnerability Analysis for 2020

See document : Critical Vulnerabilities under CVSSv2, but not CVSSv3