CVSS scoring often does not work well for DNS

Cathy Almond

2024-10-27

https://www.isc.org

What are we doing?

- Why do we issue Security Advisories?
- What do consumers of Advisories really need to know?
- What's actually worthwhile for us to be doing?

Photo by iSawRed on Unsplash

Happy Birthday CVE Program! (25 on 22nd October 2024!)

Photo by Nick Stephenson on Unsplash

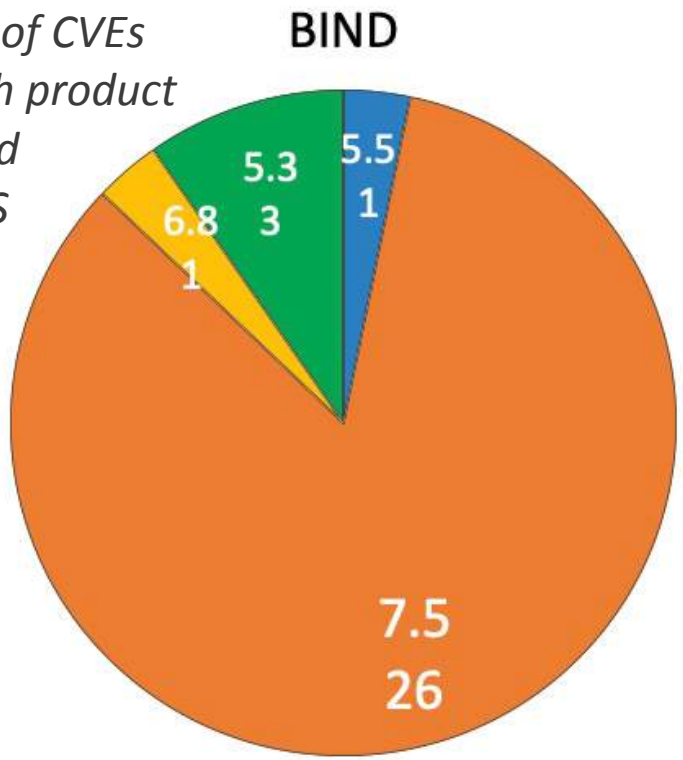
https://www.cve.org/Media/News/item/blog/2024/10/22/CVE-Program-Celebrates-25-Years

Who are the consumers of DNS Security Advisories?

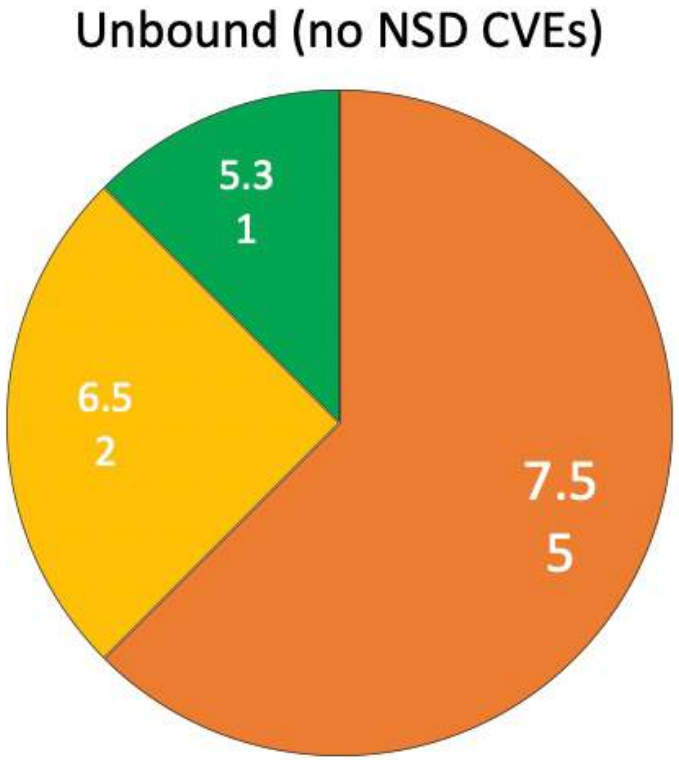
- Product users (large-scale DNS operators as well as smaller organisation system administrators)
- OS/Platform distributors and packagers
- Cyber Security Incident Response Teams (CSIRTs and similar wide-scope organisations)
- Security researchers
- The “bad guys” 

CVSS 3.1 Base scores - BIND, Unbound and Knot since January 2022

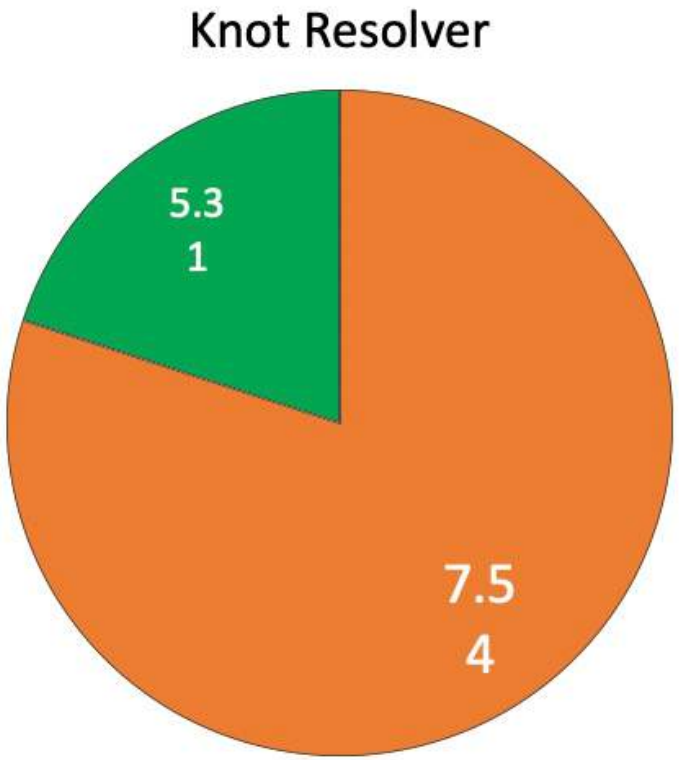
Counts of CVEs for each product grouped by CVSS score



Source kb.isc.org



Source https://www.nlnetlabs.nl/projects/unbound/security-advisories/



Source https://www.cvedetails.com/vulnerability-list/vendor_id-20536/NIC.html

KeyTrap, DNSBomb and NXNS

- KeyTrap CVE-2023-50387: CVSS 7.5
- DNSBomb CVE-2024-33655: CVSS 7.5
- NXNS
  - BIND CVE-2020-8616 CVSS: 8.6 (base)
  - Unbound CVE-2020-12662 CVSS: 7.5
  - Knot Resolver CVE-2020-12667 CVSS: 7.5
  - PowerDNS CVE-2020-10995 CVSS: 7.5

Why CVSS 7.5?

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	Adjacent Network (AV:A)	Local (AV:L)	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	Low (PR:L)	High (PR:H)

User Interaction (UI)*

None (UI:N)	Required (UI:R)

Scope (S)*

Unchanged (S:U)	Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Low (C:L)	High (C:H)

Integrity Impact (I)*

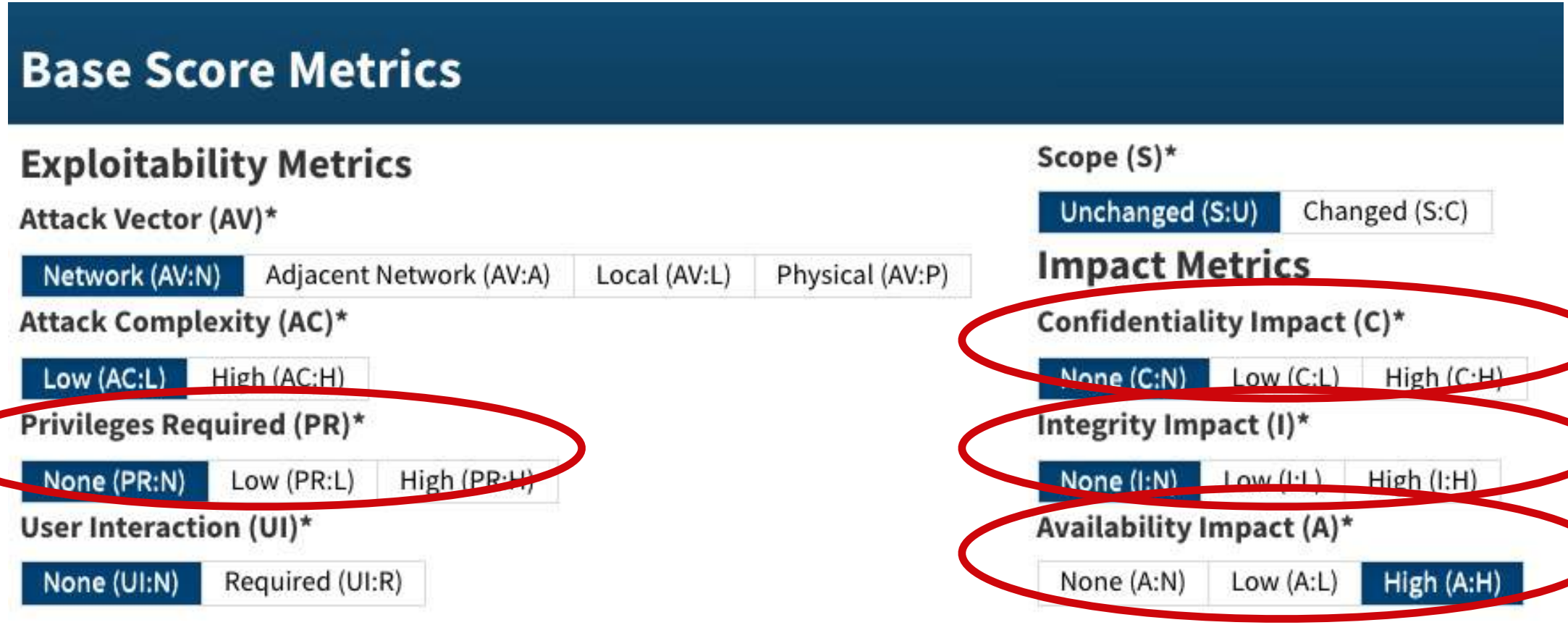
None (I:N)	Low (I:L)	High (I:H)

Availability Impact (A)*

None (A:N)	Low (A:L)	High (A:H)

Source: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H&version=3.1

Which metrics sometimes change?



Source: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H&version=3.1

Will CVSS 4.0 make a useful difference?

Photo by Dylan Hunter on Unsplash

What types of question do we receive?

- Does this affect authoritative or recursive operation?
- When/how does the vulnerability take effect?
- How likely is it that we might be affected?
- Is there a configuration or operational workaround?
- How can we mitigate this vulnerability until we can upgrade our servers?
- How quickly do we need to upgrade?
- Is my <EOL version of product> affected by this?
- *Almost no-one asks us about the actual CVSS score!*

Does identifying the CWE help?

- CWE = “Common Weakness Enumeration”
- https://cwe.mitre.org/about/new_to_cwe.html
- Probably not?

  CWE is a community-developed list of common software and hardware weakness types that could have security ramifications. A “weakness” is a condition in a software, firmware, hardware, or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities. Weakness conditions are in many cases introduced by the developer during development of the product.

KeyTrap, DNSBomb and NXNS

- KeyTrap CVE-2023-50387 CVSS 7.5 CWE-770 “Allocation of Resources without Limits or Throttling.”
- DNSBomb CVE-2024-33655 CVSS 7.5 CWE-400 “Uncontrolled Resource Consumption.”
- NXNS CWE-400 “Uncontrolled Resource Consumption.”
  - BIND CVE-2020-8616 CVSS 8.0
  - Unbound CVE-2020-12662 CVSS 7.5
  - Knot Resolver CVE-2020-12667 CVSS 7.5
  - PowerDNS CVE-2020-10995 CVSS 7.5

Source of CWE tags: https://nvd.nist.gov/vuln

Does identifying the CWE help?

- CWE = “Common W… …ation”
- https://cwe.m… …e.html
- Prob…

CWE… …ware and hardware weakn… …nications. A “weakness” is a conditio… …ware, or service component that, under ce… …uld contribute to the introduction of vulnerabi… …conditions are in many cases introduced by the developer… …velopment of the product.

CWEs appear to be more useful for researchers and software developers than for operators?

Will EPSS scores help?

- EPSS = “Exploit Prediction Scoring System”
- https://www.first.org/epss/model
- Maybe, maybe not?

  “… the output of EPSS is a probability. All we can say about vulnerability exploitation is that some of the vulnerabilities are more likely to be exploited than others, that's it, that's all EPSS is saying. EPSS is trying to provide information to practitioners that hopefully gives them an edge, that ability to play the odds and hopefully make proactive moves against attackers before they make those moves. Be careful not to compare any predictive system against perfection, instead compare against alternatives. While it'd be great to be perfect, in reality we need to identify the best strategy available to us and then try trusting it for a while.”

KeyTrap, DNSBomb and NXNS

- KeyTrap CVE-2023-50387 CVSS 7.5
  - EPSS 5.00% (Probability of exploitation activity in the next 30 days)
  - ~93% Percentile (the proportion of vulnerabilities that are scored at or less).
- DNSBomb CVE-2024-33655 CVSS 7.5
  - EPSS 0.05% (Probability of exploitation activity in the next 30 days)
  - ~14% Percentile (the proportion of vulnerabilities that are scored at or less).

NXNS *(no EPSS data)*

- BIND CVE-2020-8616 CVSS 8.0
- Unbound CVE-2020-12662 CVSS 7.5
- Knot Resolver CVE-2020-12667 CVSS 7.5
- PowerDNS CVE-2020-10995 CVSS 7.5

Source of EPSS data: https://www.first.org/epss/data_stats

(via https://www.cvedetails.com/)

Will EPSS scores help?

- EPSS = “Exploit Pr… …em”
- https://www.…
- Ma…

  “… th… …ty exploit… …exploited than oth… …g to provide informat… …edge, that ability to play the … …es against attackers before they make… …compare any predictive system against per… …against alternatives. While it'd be great to be perfect, … …to identify the best strategy available to us and then try trust… …while.”

EPSS scores are (supposedly) dynamic; but only as ‘good’ as the data available about/from the CVEs:

https://arxiv.org/pdf/2302.14172

Or there's the "just upgrade" stance?

- https://www.youtube.com/watch?v=Rg_VPMT0XXw
- If it's a bug that might be a security issue then always give it a CVE number (but not a CVSS score, although NIST may score it for you anyway)
- Guarantee backward compatibility with new releases
- Recommend always upgrade in order to be protected
- https://lore.kernel.org/linux-cve-announce/
- *That's a lot of CVEs!*

Or there's the "just up… stance?

- https://www.youtu… XXw
- If it's a bu… ways give… ough NIST…
- Guara… releases
- Recomm… to be protected
- https://lo… ve-announce/
- *That's a lo…*

But sometimes it's necessary to make potentially 'breaking' changes such as introducing new limits (for CVE-2024-1737 for example)

Multi-vendor DNS CVEs

- If a single vulnerability affects multiple products then DNS software providers will try to coordinate their security releases
- DNS-OARC Mattermost has been a very useful tool - it facilitates secure/private channels for each multi-vendor issue with representation from affected product providers (and if appropriate, researchers/reporters of issues)
- Multi-vendor security issues always don't always have the same CVE reference or CVSS score from all software providers
- Coordinated security releases are not without special challenges!

Recap: What are we doing?

- Why do we issue Security Advisories?
- What do consumers of CVEs really need to know?
- What's actually worthwhile for us to be doing?

Photo by Paul Volostnov on Unsplash

Discussion time …

Photo by Hans-Peter Gauster on Unsplash

Thank you!

- Main website: https://www.isc.org
- Software downloads: https://www.isc.org/download or https://downloads.isc.org
- Presentations: https://www.isc.org/presentations
- Main GitLab: https://gitlab.isc.org