BINDING OPERATIONAL DIRECTIVE 22-01: REDUCING THE SIGNIFICANT RISK OF KNOWN EXPLOITED VULNERABILITIES

July 13, 2022

CISA Binding Operational Directives

https://www.cisa.gov/directives

- A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.
- Section 3553(b)(2) of title 44, U.S. Code, authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives.
- Federal agencies are required to comply with DHS-developed directives.
- Issued to the head of an agency.
- These directives do not apply to statutorily defined “national security systems” nor to certain systems operated by the Department of Defense or the Intelligence Community.

Binding Operational Directive 22-01

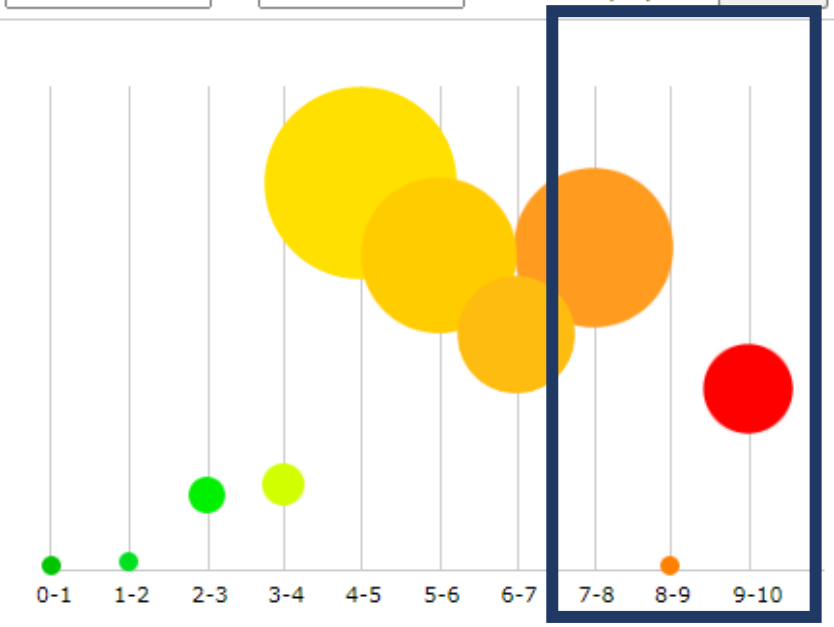
Reducing the Significant Risk of Known Exploited Vulnerabilities

- Focuses priority remediation efforts on a subset of vulnerabilities known to be exploited and posing significant risk to the Federal Enterprise.
- Enables CISA to provide continuous prioritization through a CISA managed catalog of known exploited vulnerabilities that pose a significant risk to the federal enterprise
- Requires agencies to:
  - Review and update agency internal vulnerability management procedures to align with directive requirements.
  - Remediate each vulnerability according to the timelines set forth in CISA's catalog of known exploited vulnerabilities.
  - Report on the status of vulnerabilities listed in the repository initially through CyberScope then CDM Federal Dashboard.

CVSS Scores Between 1999-01-01 and 2022-07-12

Period

1999-01-01 2022-07-12 Group By Year Submit

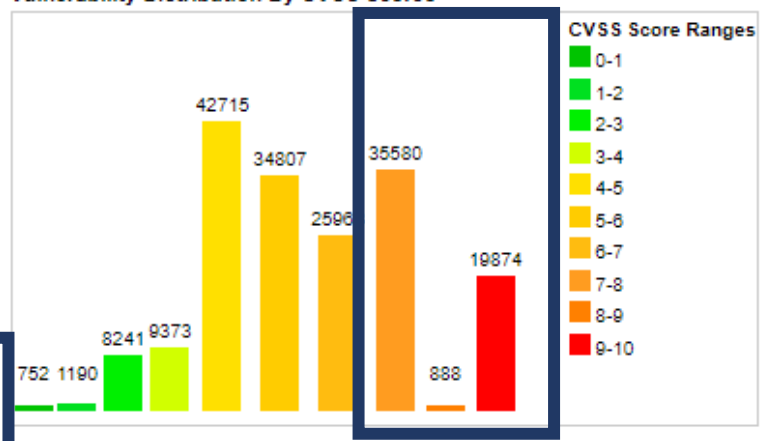


Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	752	0.40
1-2	1190	0.70
2-3	8241	4.60
3-4	9373	5.20
4-5	42715	23.80
5-6	34807	19.40
6-7	25963	14.50
7-8	35580	19.80
8-9	888	0.50
9-10	19874	11.10
Total	179383	

Weighted Average CVSS Score: 6.5

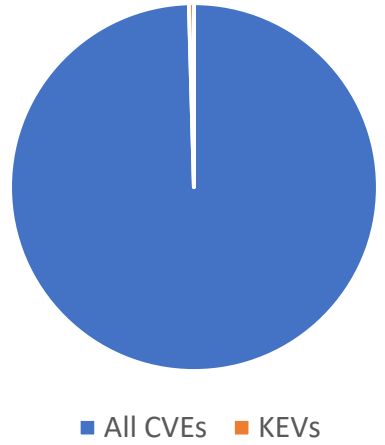
Vulnerability Distribution By CVSS Scores



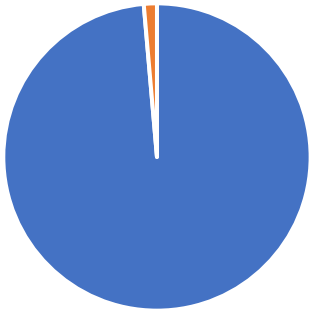
Critical (CVSS >9.0):19,874
High (7.0<CVSS<9.00): 36,468
Total Criticals and Highs: 56,342

Total KEVs: 787
(as of 7/15/22)

KEVs vs Total CVEs

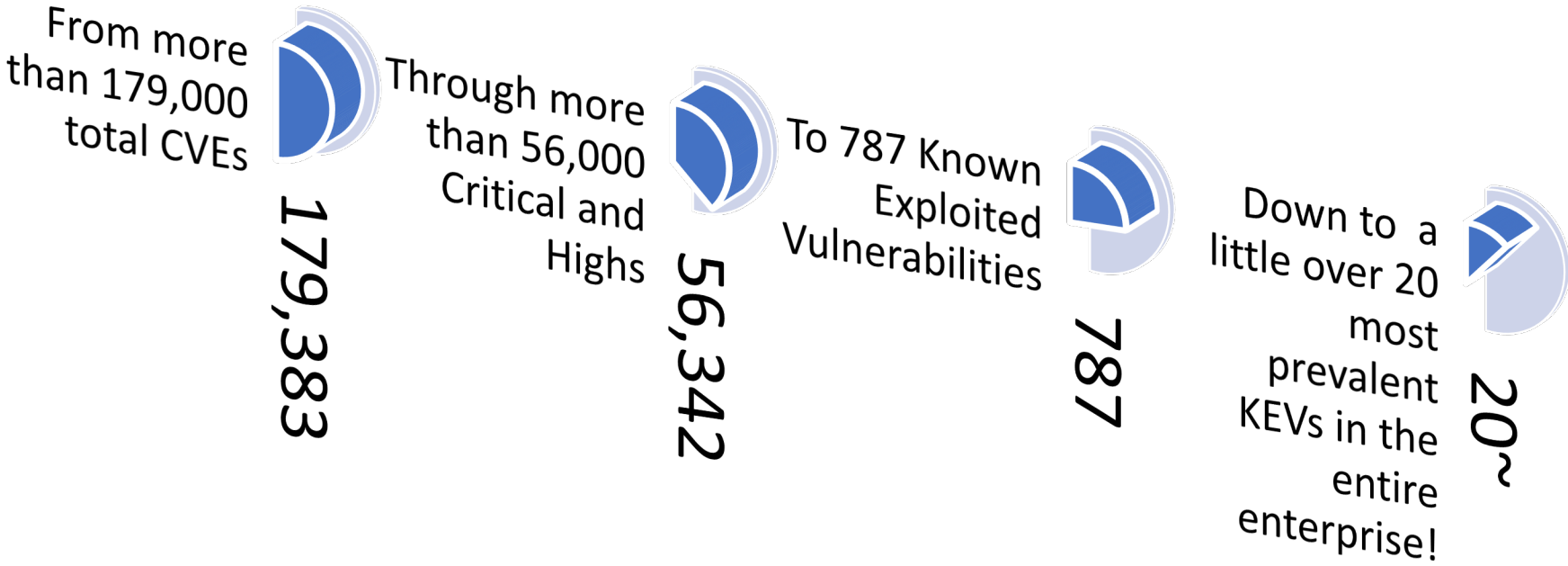


KEVs vs Critical and Highs



Source: CVSS Score Distribution Reports and Trends Over Time (cvedetails.com)

CISA has already prioritized vulnerabilities…



Timelines

- **November 17, 2021 –**
  Remediate vulnerabilities with a Common Vulnerabilities and Exposures (CVE) ID assigned in 2021 and after.
- **January 2, 2022 –**
  Update agency policies and procedures.
- **January 17, 2022 –**
  First status report due in CyberScope.
- **May 3, 2022 –**
  Remediate vulnerabilities with a Common Vulnerabilities and Exposures (CVE) ID assigned prior to 2021.
- **October 1, 2022 –**
  Reporting through CDM Federal Dashboard.

BOD 19-02:
Vulnerability Remediation Requirements for Internet-Accessible Systems

- 2 (a) Review Cyber Hygiene reports issued by CISA and remediate the critical and high vulnerabilities detected on the agency's Internet-accessible systems as follows:
- Critical vulnerabilities must be remediated within 15 calendar days of initial detection.
- High vulnerabilities must be remediated within 30 calendar days of initial detection.

Frequently asked questions

- What is the difference between vulnerabilities listed in the National Vulnerability Database (NVD) and those in CISA's catalog of Known Exploited Vulnerabilities (KEVs)?
- What is more important to remediate first - critical and high or Known Exploited Vulnerabilities?
- With extended telework, most of our workstations are remote and hard to patch, does CISA have any recommendations for patching roaming and nomadic devices?
- How often will CISA add new vulnerabilities to the catalog?
- What's the difference between a High or Critical CVE and a Known Exploited Vulnerability (KEV)?
- Aren't agencies already required to patch against all CVEs? What's the point of creating a new patching requirement? Should my organization still use CVSS for prioritization?
- How should agencies report vulnerabilities in federal information systems hosted in third-party environments (such as the Cloud)?
- This is a comprehensive catalog of vulnerabilities that carry unacceptable risk to the federal enterprise. Will that information be shared in some manner with the public and private sector?

Resources

Please share this information widely and reach out for assistance or if you have questions

- Questions about CISA's Binding Operational Directives and Emergency Directives, including the Catalog of Known Exploited vulnerabilities:
  CyberDirectives@cisa.dhs.gov
- All other questions about CISA, services available to government agencies, etc.:
  CyberLiaison@cisa.dhs.gov
- CISA Cyber Directives
  https://cisa.gov/directives
- Catalog of Known Exploited Vulnerabilities
  https://www.cisa.gov/known-exploited-vulnerabilities


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY