Recorded Future

REPORT

The Dragon Is Winning

U.S. Lags Behind Chinese Vulnerability Reporting

By Dr. Bill Ladd
Chief Data Scientist
Recorded Future

CTA-2017-1019

Table of Contents

Executive Summary....4

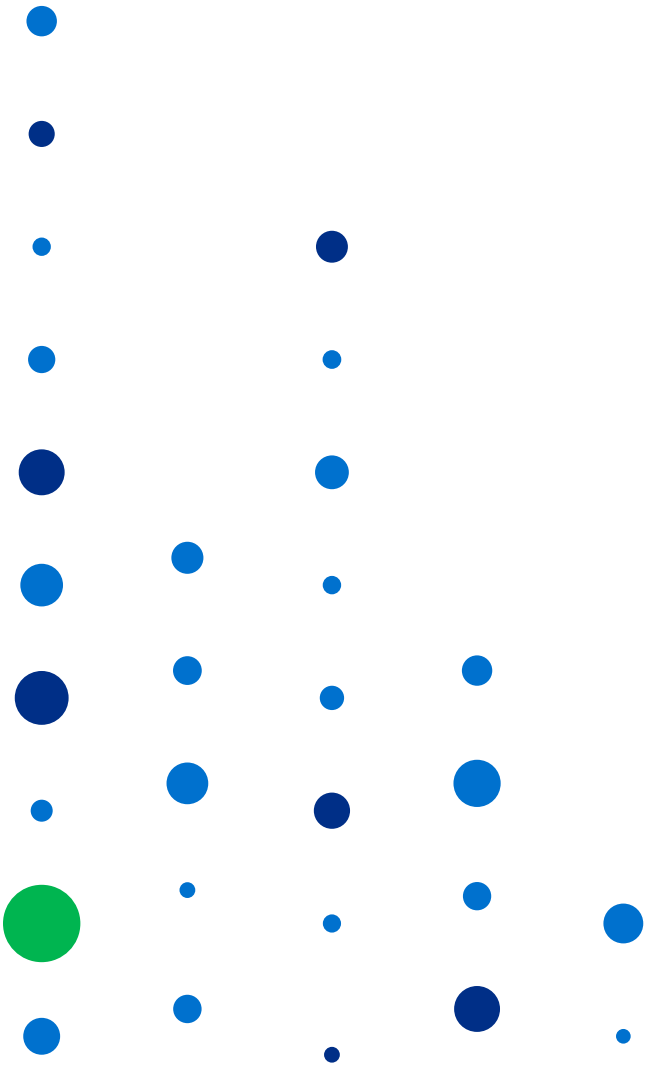
Background....4

Analysis....5

Why Is NVD so Slow?....7

Chinese Vulnerability Reporting....9

Conclusion....10



Recorded Future

Executive Summary

- Organizations need access to the latest vulnerability (CVE) information to manage their exposure to risk.
- The U.S. National Vulnerability Database (NVD) trails China's National Vulnerability Database (CNNVD) in average time between initial disclosure and database inclusion (33 days versus 13 days).
  - China isn't directly integrated in managing CVEs, but are still able to report vulnerabilities more rapidly than the U.S.
- CNNVD actively gathers vulnerability information across the web. NVD should do this but instead waits for voluntary submission by vendors.
- NVD's mission should aim to be truly comprehensive, and the U.S. could improve by simply incorporating content from China's CNNVD.
  - 1,746 CVEs are currently in CNNVD and absent in NVD.

Vulnerabilities are continuously found in all software and organizations need access to the latest vulnerability information to manage their exposure to risk. Because organizations use systems provided by dozens of software vendors, they require access to a centralized source of vulnerability information across all vendors to prioritize which to address next.

Background

In prior research we took a close look into software vulnerability (CVE) disclosure and learned that there were unexpectedly large gaps between public disclosure of a vulnerability and inclusion in the U.S. National Vulnerability Database (NVD). Concerned about this performance, we compared NVD CVE reporting times to what we observe on China's National Vulnerability Database (CNNVD).

Scope Note: *We examined how many days after initial web disclosure NVD and CNNVD waited to report the 17,940 vulnerabilities first publicly disclosed and then incorporated by both systems between September 13, 2015 and September 13, 2017. Initial web disclosure includes any mention of the vulnerability on the web. Our dataset is based on Recorded Future holdings.*

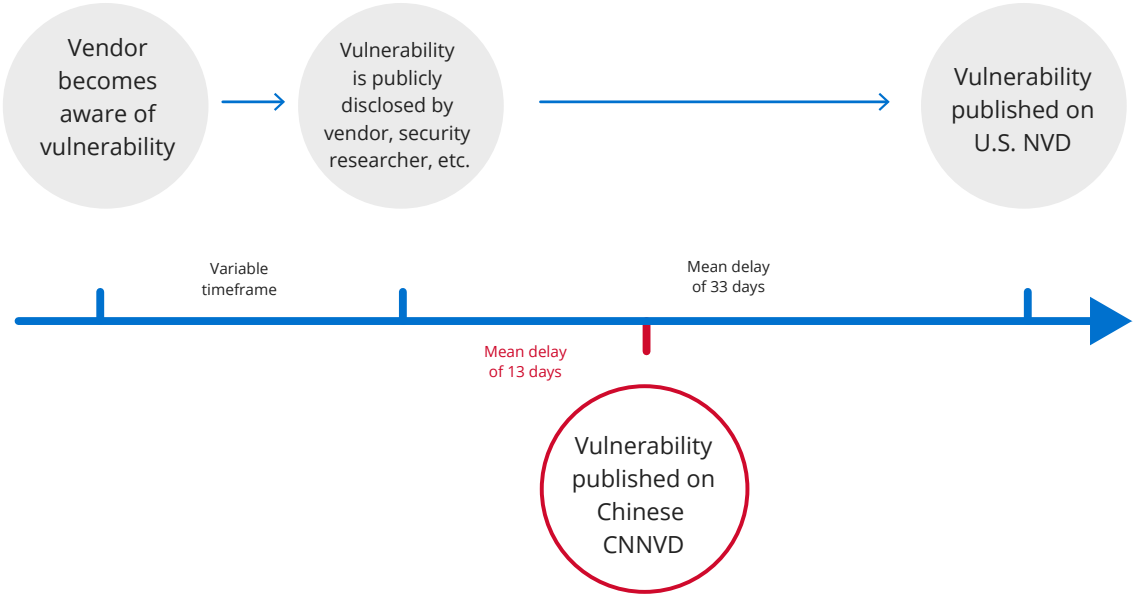
Home pages of NVD and CNNVD.

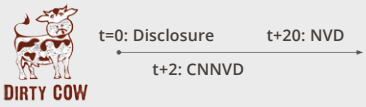
Analysis

CNNVD outperforms NVD in reporting vulnerabilities.

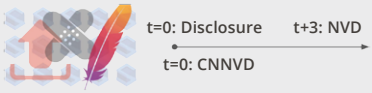
On any given day, there is more current information about software vulnerabilities on CNNVD than on NVD. We found an average delay between first disclosure and availability on CNNVD of 13 days. On NVD, the average delay is 33 days.

Vulnerability Reporting Timeline





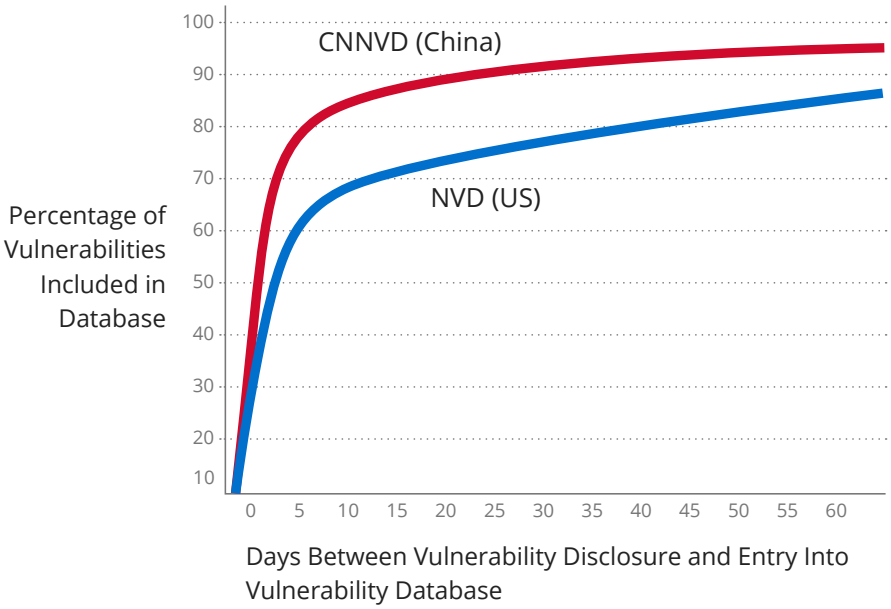
Reporting delays give adversaries a head start over defenders. Privilege escalation vulnerability CVE-2016-5195, commonly referred to as Dirty Cow, was detected by researchers analyzing active exploits and disclosed on October 19, 2016. It was immediately covered by numerous information security sources and within two days, an initial report was translated to Russian and posted on a Russian criminal forum. Six days later, POC code was placed on Pastebin. This potential exploit code was available a full two weeks before the November 10 initial release for this CVE on NVD. CNNVD reported on this vulnerability two days after initial disclosure, 20 days before NVD.



Even smaller delays can be important for critical bugs. CVE-2017-5638, the vulnerability responsible for the Equifax breach, was first announced by the Apache Software Foundation on March 7, 2016. It was immediately picked up by numerous sources and we saw hundreds of reports between March 7 and March 10 when it was included in the NVD database. Two places we observed it on release day March 7 were CNNVD and a Chinese blog that included POC code.

Averages can be dominated by a small set of vulnerabilities with long delays, so we looked at the data based on percentiles as well. Within six days of initial disclosure, 75 percent of all vulnerabilities published on the web are covered in CNNVD. The U.S. NVD takes 20 days.

CNNVD captures 90 percent of all vulnerabilities within 18 days. The NVD takes 92.



There are two classes of vulnerability disclosure: coordinated and uncoordinated. In some cases, a vendor clearly coordinates the announcement of the vulnerability, and it is simultaneously publicly disclosed and reported in NVD. In these cases CNNVD trails NVD by a median of one day. When the vendor doesn't tightly coordinate with NVD, it takes NVD 38 days to report on 75 percent of published vulnerabilities and 125 days to cover 90 percent. For CNNVD in these cases it takes seven days to report on 75 percent and 23 days to report on 90 percent.

Why Is NVD so Slow?

NVD publication delays of weeks and months occur because NVD is waiting for the voluntary submissions of information. To better understand why, we need to understand the groups involved. NVD is managed by the Security Testing, Validation, and Measurement Group of the Information Technology Laboratory of the National Institute of Standards and Technology (NIST). The NIST overview of NVD states:

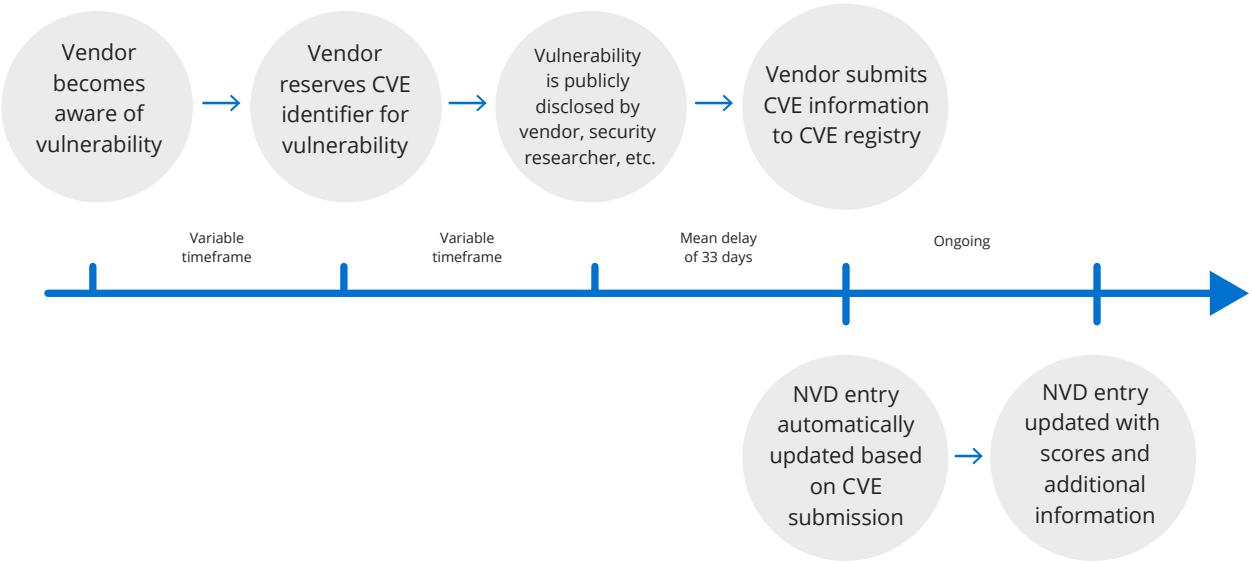
"NVD is a comprehensive cyber security vulnerability database that integrates publicly available U.S. government vulnerability resources and provides references to industry resources."

At first glance this seems reasonable — comprehensive coverage including information from industry resources. Looking a little deeper on the NVD website we see:

"The NVD performs analysis on CVEs that have been published to the CVE Dictionary. NVD staff are tasked with analysis of CVEs by aggregating data points from the description, references supplied and any supplemental data that can be found publicly at the time."

Essentially the NVD is reporting and analyzing vulnerabilities only after they are published in MITRE Corporation's CVE Dictionary. If the CVE is not published in the CVE Dictionary, it's not included in NVD nor available to companies relying on NVD for vulnerability awareness.

CVE Submission Process



NVD Process

Taking a closer look at MITRE, it is readily apparent that MITRE does not simply maintain the CVE Dictionary, they oversee the entire CVE process including the selection and management of "CVE Numbering Authorities" (CNAs).

From their website:

"The MITRE Corporation maintains CVE and this public website, oversees the CNAs and CVE Board, manages the compatibility program, and provides impartial technical guidance throughout the process to ensure CVE serves the public interest."

Oracle, for example, is a CNA with the ability to generate CVE identifiers for vulnerabilities found in Oracle products. A CNA such as Oracle identifies a vulnerability in their software and assigns a CVE. They then typically disclose information about the vulnerability, potential impact, affected products, and available patches in a security bulletin on their website. Ideally the CNA would simultaneously update the CVE Dictionary thus leading to the addition of the vulnerability to NVD. At this point, our analyses show that the system breaks down as CNAs do not typically update MITRE's CVE Dictionary in a coordinated fashion.

NVD publication delays of weeks and months occur because NIST and MITRE are waiting for the voluntary submissions of the vendors and CNAs associated with the vulnerabilities. MITRE manages the process, but doesn't enforce timely submissions to the CVE Dictionary. NVD uses the CVE Dictionary as its sole source. The end result is that there is no U.S. government "comprehensive cybersecurity vulnerability database."

Chinese Vulnerability Reporting

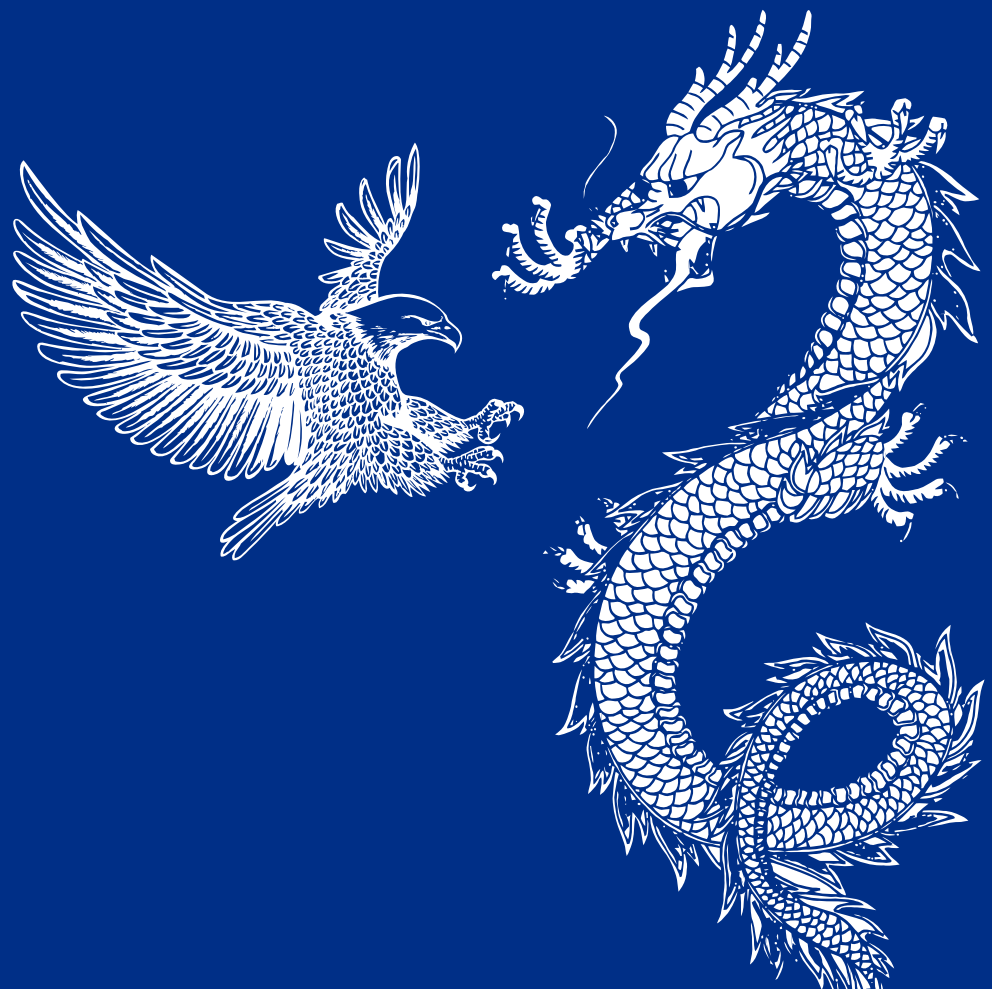
China's CNNVD doesn't have the luxury of being directly integrated in the exact processes that assign CVE numbers, but they are still able to report more rapidly than the U.S. As we saw in our earlier reporting there are numerous sources reporting on software vulnerability in advance of NVD publication. The only way to stay current is to monitor these varied sites either manually or using automated processes. Translated from the CNNVD website:

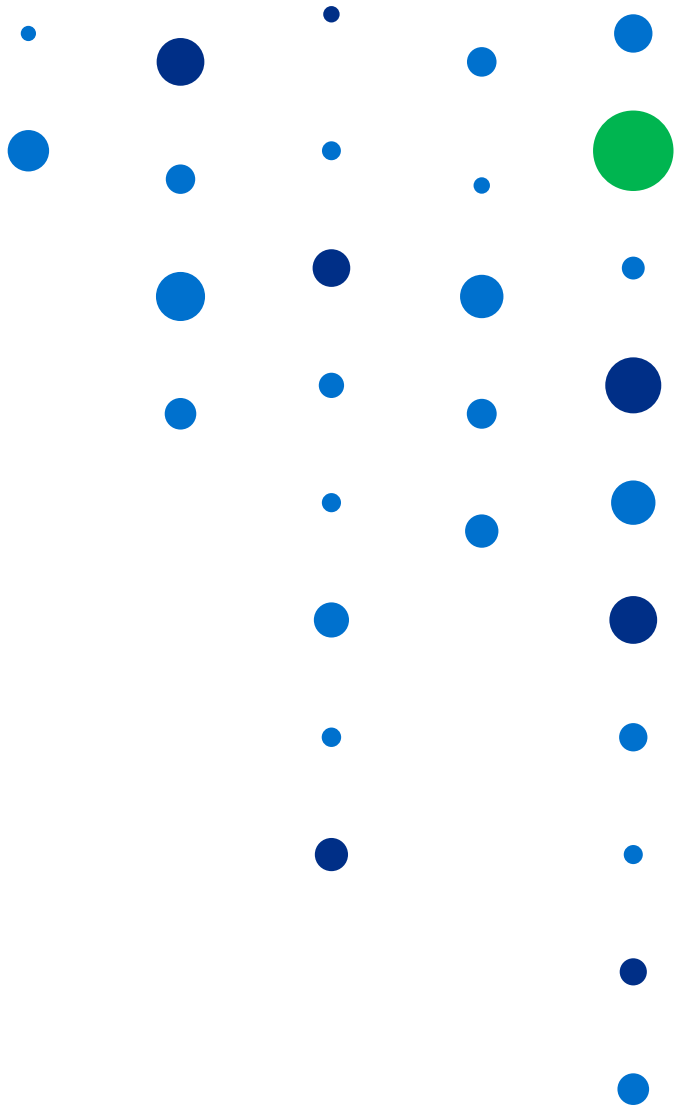
"CNNVD is … responsible for the construction of, operation, and maintenance of national information security vulnerability data management platform … through independent mining, social submission, collaboration and sharing, network collection and technical testing, joint government departments, industry users, security vendors, universities and research institutions and other social forces …"

China has prioritized timely disclosure by using extensive sources of vulnerability information across the web rather than relying on voluntary industry submissions. While the U.S. government has focused on a process, China has focused on the key goal, reporting available vulnerabilities. Surely NIST's Information Technology Laboratory, with its ~400 scientific and technical staff and its ~$120 million budget could do the same. Or at worst, assign interns to capture what is found on CNNVD and incorporate into NVD. They could start with the 1,746 CVEs currently available in CNNVD and unavailable on NVD.

Conclusion

When hackers and security teams are racing to exploit or patch vulnerabilities, having access to the latest vulnerability information is critical. The United States National Vulnerability Database (NVD) is an obvious place security teams should be able to rely on to get this latest information. Unfortunately, because NVD relies on voluntary submissions, NVD is often updated weeks after a vulnerability is initially disclosed. This gap ensures that NVD cannot provide comprehensive vulnerability coverage. NVD should extend its mission to proactively gather vulnerability information as its Chinese counterpart (CNNVD) does. Blackhat hackers who monitor the CNNVD could benefit from its more complete collection as they are looking for new exploits to target. U.S. security teams should have access to a similar resource.





Recorded Future

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with threat intelligence powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context that's delivered in real time and packaged for human analysis or instant integration with existing security technology.