Recorded Future

REPORT

China's Ministry of State Security Likely Influences National Network Vulnerability Publications

By Priscilla Moriuchi and Dr. Bill Ladd

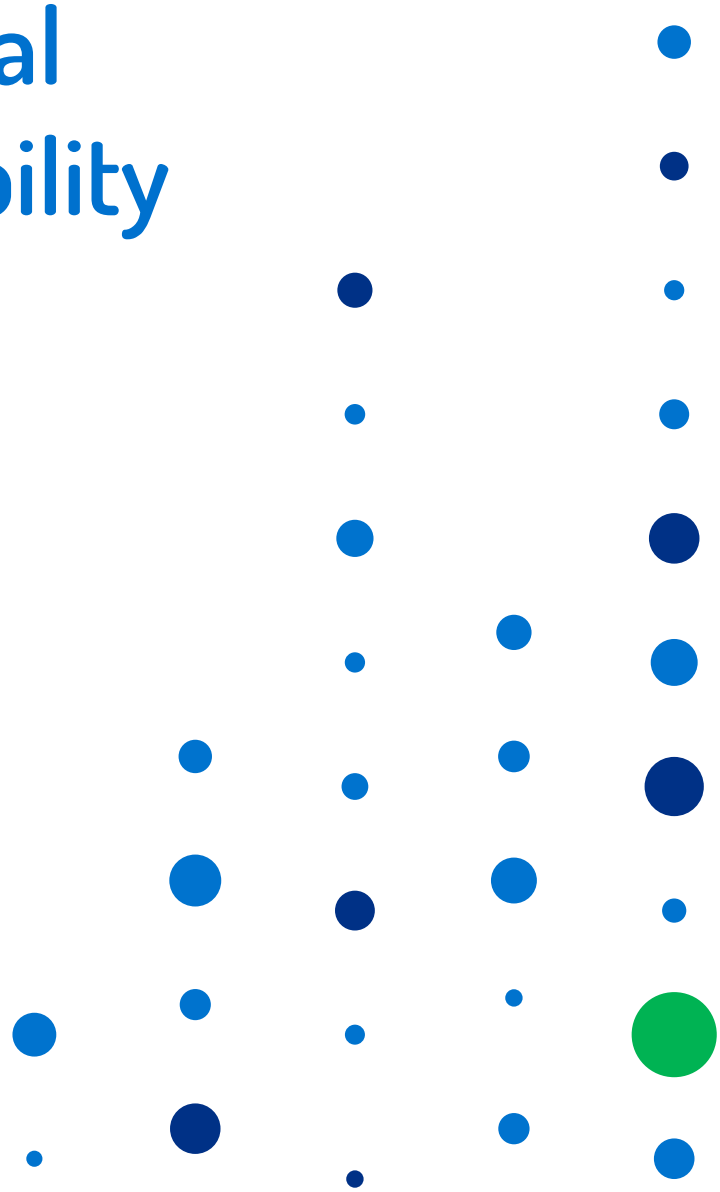
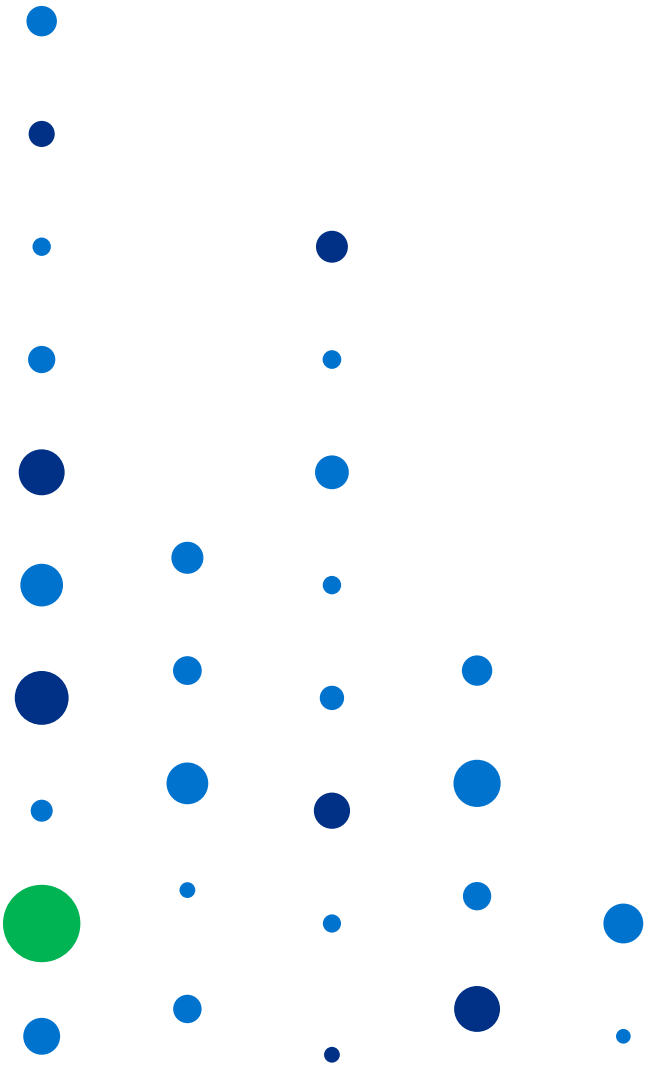


Table of Contents



Recorded Future

Executive Summary

Earlier research based on the last two years of vulnerability reporting illustrated that China's National Vulnerability Database (CNNVD) was generally more aggressive in capturing up-to-date information for software vulnerabilities than its U.S. counterpart (NVD). In this research we examine exceptions to this general rule and discover a broader role for the Ministry of State Security (MSS) in vulnerability reporting than was previously known.

Recorded Future analysis has uncovered evidence of a formal vulnerability evaluation process at CNNVD in which High-threat CVEs are likely evaluated for their operational utility by the MSS before publication.

We studied 300 CVEs, representing CVE 1) with the most atypical CNNVD reporting delays and 2) associated with malware used by Chinese APT, and discovered multiple examples where we believe the MSS may have delayed the publication of High-threat vulnerabilities.

- In one instance, a Chinese APT group was actively exploiting the Microsoft Office vulnerability (CVE-2017-0199) during the publication lag of 57 days after NVD published.
- The most atypical publication delay experienced by CNNVD (236 days), was for a pre-installed backdoor that sent vast amounts of user data to servers in China and was possibly associated with Chinese government surveillance.
- Among groups of vulnerabilities that were released together, High-threat vulnerabilities were consistently published substantially later (anywhere from 21 to 156 days later) than Low-threat vulnerabilities.

Further, our research on vulnerabilities commonly exploited by malware linked to Chinese APT groups revealed an inconsistency in CNNVD publication practices. CNNVD breaks its larger pattern and is beat to publication by NVD on 97 percent of these vulnerabilities. *The probability that NVD would beat CNNVD to publication for this proportion of CVEs is incredibly small — less than .00001 percent.* We believe CNNVD publication was likely delayed by the MSS because Chinese APT groups were actively exploiting those vulnerabilities.

Lastly, we discovered that on average, it takes CNNVD longer to publish vulnerabilities with High Common Vulnerability Scoring System (CVSS) scores than vulnerabilities with Low ones. This is in contrast to NVD, which publishes High CVSS vulnerabilities more quickly than lower ones.

We assess that this is likely due to influence by the MSS in delaying the publication of High-threat vulnerabilities in order to evaluate its utility in future intelligence operations or buy time for current ones.

Key Judgments

- CNNVD is essentially a shell for the MSS; it has a website but appears to be separate from the MSS in name only.
- We have identified at least two examples of vulnerabilities with CNNVD publication delays that we believe were likely influenced by the MSS.
- Even though CNNVD beats NVD to publication 43 percent of the time, for vulnerabilities exploited by malware linked to Chinese APT groups, CNNVD was first to publish for only three percent of those.
- It takes CNNVD longer to publish vulnerabilities with high CVSS scores than low ones, even though there is no increase in published context, indicating that there might be different reporting and evaluation procedures for high-threat vulnerabilities.
- For a small subset of vulnerabilities (44 CVEs), NVD is faster than CNNVD to publish vulnerabilities that already have exploits for them.

Background

As we previously reported in "The Dragon Is Winning," the U.S. NVD trails China's National Vulnerability Database (CNNVD) in average time between initial vulnerability disclosure and database inclusion. On average, it takes the U.S. NVD 33 days after public disclosure to make a vulnerability available in its database, while it takes CNNVD only 13 days. Further, CNNVD captures 90 percent of all vulnerabilities within 18 days; it takes the NVD 92 days to cover that same percentage.

The explanation for the delay by NVD is relatively simple — NVD waits for voluntary submissions of information, while CNNVD pulls data from 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 — quickly reporting available vulnerabilities.

For this research, we studied two groups of CVEs. The first, was a statistically unique subset (268 CVEs) of the 17,940 vulnerabilities first publicly disclosed and then incorporated by both NVD and CNNVD between September 13, 2015 and September 13, 2017. This subset were of CVEs that were reported quickly by NVD and slowly by CNNVD. We know from our previous research that NVD prioritizes significant vulnerabilities for faster release; therefore, when we see CVEs published quickly by NVD followed by a long CNNVD lag, it is extremely atypical. We hereafter refer to these CVEs as the "outliers."

Our second group of CVEs were of vulnerabilities exploited by malware used by Chinese APT groups. We studied 15 different pieces of malware used by Chinese APT groups, which included 32 separate CVEs. In total, we studied 300 different CVEs for this research.

CNNVD: Thinly Veiled Front Organization for the MSS

As we identified in additional previous research, CNNVD is run by the China Information Technology Evaluation Center (CNITSEC), which is an office in China's premier foreign intelligence service, the Ministry of State Security (MSS). Further research into the administration of CNNVD has revealed that it is essentially a shell, or cover, for the MSS.

Submissions to CNNVD are directed to vulpro@itsec.gov.cn, which is CNITSEC's domain, as are all contact email addresses (that we could discover) for CNNVD.

Vulnerability submission page for CNNVD.

Further, the location and contact information for both CNITSEC and CNNVD are identical. Both are located in the same building, on the same floor, and have the same contact phone numbers.

Contact information for CNITSEC and CNNVD; both list the same contact phone numbers and address.

The MSS runs CNNVD. The closest U.S. analog to the MSS is the Central Intelligence Agency (CIA), and the MSS running the CNNVD is the equivalent of the CIA running the NVD. Conversely, the CIA does not run the U.S. NVD; it is run by a division within the Department of Homeland Security (DHS) tasked with publicly identifying, reporting, and creating patches for software vulnerabilities. While there is not an exact DHS equivalent in China, the Ministry of Public Security (MPS) mission and scope is most similar and is widely considered China's DHS counterpart.

The fundamental problem with the MSS running CNNVD, and more broadly, the MSS's role in China's information security architecture, is that the MSS is China's "leading civilian intelligence agency," responsible for both foreign intelligence and counterintelligence operations. This means that the MSS could use the information gained from vulnerability submissions to CNNVD to then exploit in its own intelligence operations. The MSS has a voice in which vulnerabilities are reported via the CNNVD, because they run it; they could also easily identify and hide from the public a critical weakness in software or hardware, then turn around and use it in its own operations.

Shared location of CNITSEC and CNNVD.

It is this relationship, where the public defensive mission is supervised by an intelligence service with broad powers to collect intelligence both domestically and overseas, that led us to investigate CNNVD statistical reporting anomalies in greater depth.

What is the influence of the MSS on CNNVD, the publishing of vulnerabilities, and public information security in China?

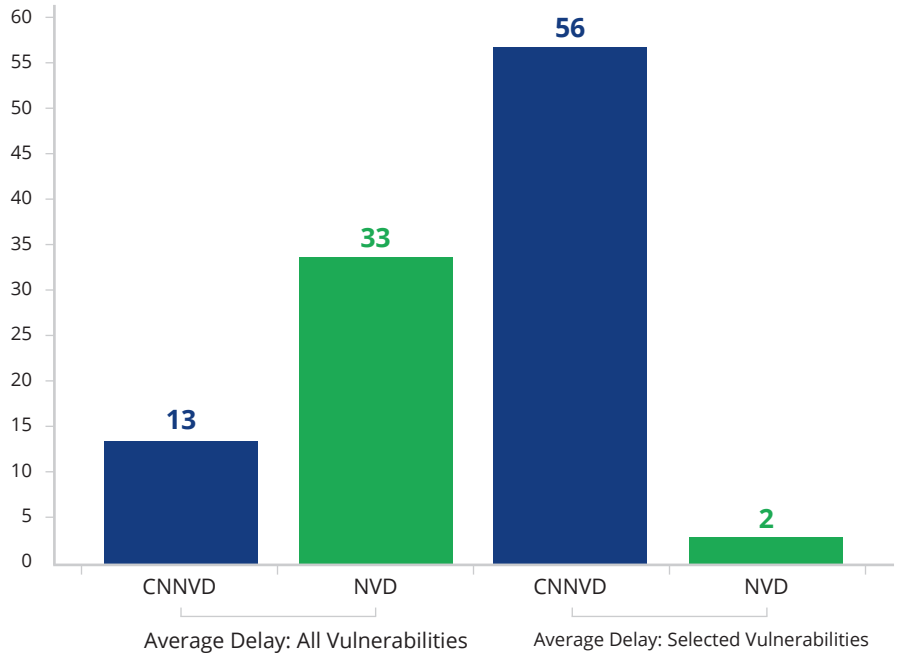
Threat Analysis

In examining the outliers, two analytic questions jumped out from the data. What can we learn from the CVEs that 1) experienced large lags in publishing, and 2) are associated with malware commonly used by Chinese state-sponsored groups?

Large Lags in Publishing

For the outliers, we decided to examine CVEs NVD reported on quickly (six days or less) and that CNNVD took over twice as long as its average delay of 13 days to publish. This length of delay (we selected 28 days, or four weeks) is a full 10 days longer than the 90 percent publishing rate and should control for the typical organizational and bureaucratic issues and delays, like employee vacation, national holidays, systems or network problems, etc.

Out of the 17,940 vulnerabilities first publicly disclosed and then incorporated by both NVD and CNNVD between September 13, 2015 and September 13, 2017, *268 vulnerabilities (or approximately 1.5 percent) took less than six days for NVD to publish and longer than 28 days for CNNVD to publish.*



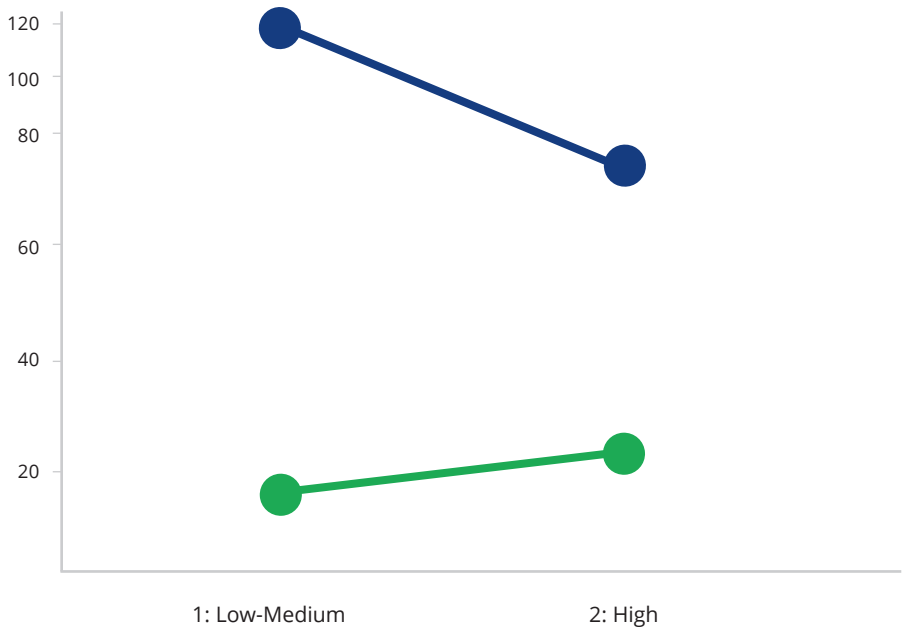
Average reporting delays for all vulnerabilities in time frame and the selected set of vulnerabilities used in this analysis.

Of these 268, nearly 43 percent had a Common Vulnerability Scoring System (CVSS) severity rating of High, 45 percent had a Medium CVSS rating, and 12 percent were Low.

When these vulnerabilities are broken down further by published date, the data follows a similar pattern. The vast majority of the delayed vulnerabilities (74 percent) were published 28 to 50 days after initial report; however, 11 percent were published in 51 to 91 days, and 15 percent took over 120 days to publish.

Additionally, there were several companies and projects with numerous vulnerabilities among these outliers, with the largest numbers being from Cisco, Oracle, Linux, Adobe, Google, IBM, and Microsoft, in sequential order.

As we identified in prior research, for the NVD, higher-severity vulnerabilities have shorter release lags as more effort is put into communicating and remediating them. However, for CNNVD, the opposite is true. On average, CNNVD takes three days longer to report a vulnerability with a High score than a Low-Medium score.



Severity scores of vulnerabilities vs. lag until 90 percent vulnerability coverage. NVD (blue) is faster in publishing high-severity vulnerabilities than lower-severity vulnerabilities; CNNVD (green) is slower to publish high-severity vulnerabilities than lower-severity vulnerabilities. Overall CNNVD is still faster.

The diverging trend lines in responsiveness to more severe vulnerabilities raise interesting questions about reporting criteria and priorities. While CNNVD is still faster than NVD in each CVSS category, NVD is fastest when reporting High vulnerabilities, while High is CNNVD's slowest category. Further, of the selected outliers, 43 percent were High even though these vulnerabilities make up only about one-third of all total published vulnerabilities. The probability of this degree of difference occurring by chance is quite small, 0.016 percent.

Why is this the case? Does CNNVD publish more content on High and Medium vulnerabilities than on Low ones? What could account for this systemic lag in publishing more severe vulnerabilities, or the fact the nearly 43 percent of the statistical outliers had High CVSS scores?

A Tale of Two Vulnerabilities

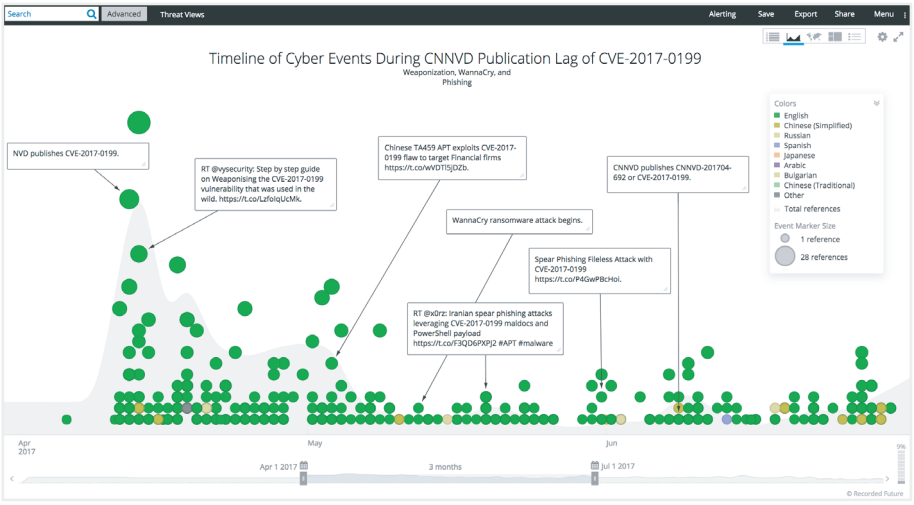
In addition to our NVD comparisons and statistical modeling, we decided to compare NVD and CNNVD publish dates and content for two High vulnerabilities: CVE-2017-0199 and CVE-2016-10136/CVE-2016-10138.

1. CVE-2017-0199 is a Microsoft Office vulnerability that was first identified on April 11, 2017. In the succeeding months, this vulnerability was successfully exploited by North Korean state-sponsored actors in the global WannaCry attack, the unknown actors responsible for NotPetya, and the criminal group behind Dridex. This vulnerability was widely exploited across the world, including in China.

Below are side-by-side screenshots of the U.S. NVD and CNNVD entries for CVE-2017-0199 (CNNVD assigns its own numbers and calls this one CNNVD-201704-692).

Both NVD and CNNVD contain brief descriptions of the vulnerability, version affected, and links to the security patch. Interestingly, CNNVD's entry contains fewer references, technical details, and does not list the original identification date (April 11), only the dates which CNNVD published and updated the entry (both June 7, 2017). CNNVD links to the MITRE maintained CVE entry and the description of the vulnerability on CNNVD appears to be very similar to the MITRE description.

In comparing the content of both NVD and CNNVD entries for this vulnerability, there is no evident explanation as to why CNNVD took 57 days after disclosure to publish. There is no additional content or analysis in CNNVD's entry. Aside from having a different vulnerability number and risk class score (although it was still the highest category so it was virtually the same), CNNVD actually had less useful data on this particular entry.



Timeline of cyber events during CNNVD publication lag of CVE-2017-0199.

However, for this particular vulnerability, there may have been other influencing factors which drove the publication lag. Research published on April 27, 2017, revealed that a suspected Chinese APT group, referred to as TA459, had been using this vulnerability to target analysts who covered the telecommunications industry at Russian and Central Asian financial firms. This group has also utilized a number of other tools commonly associated with Chinese APT groups, such as PlugX, NetTraveler, and Gh0st. In this case, TA459 had been using a trojan called ZeroT to exploit CVE-2017-0199.

Given that the MSS runs CNNVD, it is likely that the publication lag for CVE-2017-0199 could have been affected by the MSS which wanted to buy time for the vulnerability to be exploited in its operations or on behalf another Chinese state-sponsored actor.

2. CVE-2016-10136 and CVE-2016-10138 are two vulnerabilities in Android software developed by a company named Shanghai Adups Technology. According to Kryptowire, these two vulnerabilities are essentially pre-installed backdoors which, "actively transmitted user and device information including the full-body of text messages, contact lists, call history with full telephone numbers, unique device identifiers including the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI). The firmware could target specific users and text messages matching remotely defined keywords. The firmware also collected and transmitted information about the use of applications installed on the monitored device, bypassed the Android permission model, executed remote commands with escalated (system) privileges, and was able to remotely reprogram the devices."

The New York Times wrote a profile of the two vulnerabilities on November 15, 2016, stating that, "the Adups software transmitted the full contents of text messages, contact lists, call logs, location information, and other data to a Chinese server. The code comes pre-installed on phones and the surveillance is not disclosed to users." The article went on to connect the Shanghai Adups-developed backdoor to Chinese government surveillance.

> *"The episode shows how companies throughout the technology supply chain can compromise privacy, with or without the knowledge of manufacturers or customers. It also offers a look at one way that Chinese companies — and by extension the government — can monitor cellphone behavior. For many years, the Chinese government has used a variety of methods to filter and track internet use and monitor online conversations. It requires technology companies that operate in China to follow strict rules."*

Below are screenshots of the NVD and CNNVD entries for CVE-2016-10136 (CNNVD number CNNVD-201701-365).

Similar to the entries for CVE-2017-0199, each includes a brief description of the vulnerability and links to references. The CNNVD entry, however, contains significantly less detail about the vulnerability itself and includes only a generic and misrepresentative statement about the risk to users. "A local attacker could exploit this vulnerability to read, write, and delete files, and to gain additional privileges."

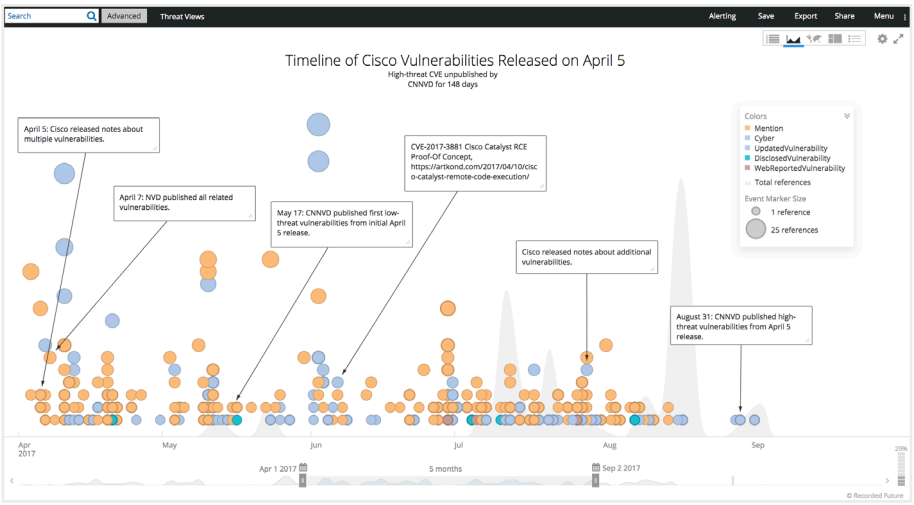
Additionally, CNNVD published this sparse writeup over eight months (236 days) after NVD, and nearly 10 months after the vulnerability was initially exposed. Based on CNNVD's statistical average for publishing vulnerabilities with High CVSS scores (90 percent of High vulnerabilities are published within 20 days), the breadth of its source material, and the limited text in the entry itself, this is another case where the extended delay in publication is unexplainable.

It is likely that CVE-2016-10136 and CVE-2016-10138 are another example of MSS leveraging its authority over CNNVD on behalf of its operations. This publication lag of 236 days was the longest delay for a vulnerability published by CNNVD. We do not believe that these vulnerabilities, the links they might have to Chinese government surveillance, and the eight month publication delay are coincidences. The systems with these backdoors were overwhelmingly located in China, CNNVD is largely followed and consumed by Chinese businesses and citizens, and the MSS has a mission to collect domestic intelligence. While we cannot determine with certainty that the MSS was exploiting this vulnerability, we believe this is another example of likely MSS interference in the CNNVD publication process.

Groups of CVEs Within the Outliers

Further, CVE-2017-0199 was part of a group of vulnerabilities published and patched by Microsoft on April 11, 2017. Some of the other CVE contained in this April 11 update included CVE-2017-0158, CVE-2017-0164, CVE-2017-0167, CVE-2017-0181, and CVE-2017-0207. CVE-2017-0164 and CVE-2017-0167 both had low CVSS score (3.5 or less) and were published by CNNVD in 36 days, while the other four had medium or high CVSS scores and were not published for an additional 21 days (57 days total).

Among these outliers, we identified two other groups of vulnerabilities where CNNVD handled publication in a similar manner. On April 5, 2017, Cisco released security notes about multiple vulnerabilities, all of which were published by NVD within two days, but in CNNVD 42 and then 148 days later. The low CVSS score vulnerabilities were published in 42 days and the medium and high vulnerabilities in 148 days.



Timeline of Cisco vulnerabilities released on April 5.

The other group was a series of Linux vulnerabilities, published in an Android Security Bulletin on April 1, 2017. Again, each CVE in this set was published by NVD within four days, but published by CNNVD in 44 to 156 days, with the higher CVSS score vulnerabilities being published later.

We believe this dissimilar treatment of vulnerabilities within each group of CVEs is another indicator that CNNVD has a different process for publishing vulnerabilities that may have operational use for the MSS.

CVEs Exploited by Chinese APT Groups

To address the second question regarding how CNNVD treats vulnerabilities that are commonly exploited by malware linked to Chinese APT groups, we examined CVEs that were exploited by 15 different pieces of malware. These included:

- 9002RAT
- BS2005
- Derusbi
- FakeM
- Pirpi
- PoisonIvy
- Sakula
- Sykipot
- Sysget
- ZeroT
- ZoxPNG
- BBSRat
- ZxShell
- IsSpace/Nflog
- TidePool

Note: These malware represent only a subset of exploits used by Chinese APT groups. We selected these because they represent a wide range of exploits, from more niche to broader, publicly accessible tools.

The 15 pieces of malware exploited 32 different vulnerabilities (full list is in Appendix A). Thirty-one of these vulnerabilities were published by NVD first; the only one published first by CNNVD was CVE-2007-0671. NVD published 31 vulnerabilities within one day of disclosure, the other was published three days later.

CNNVD published 93 percent (30) of these exploited CVEs within six daysof disclosure. The other two vulnerabilities were published after 12 (CVE-2013-1347, utilized by PoisonIvy) and 56 days (CVE-2017-0199, utilized by ZeroT, also see section above).

Given that CNNVD beats NVD to publication 43 percent of the time, we should expect to see about 13 of these vulnerabilities reported by CNNVD first, however, we see only one. That one represents only three percent of these CVEs and is far outside of the statistical norm.

As a comparison, we studied 13 CVEs exploited by malware linked to the NSA-associated Equation Group. Although a smaller sample size, it proves a useful foil in that 11 of the vulnerabilities were reported by NVD first, two by CNNVD.

All CVEs were reported by NVD within three days except one, CVE-2017-0176, which was published after nine days (CNNVD published this vulnerability in one day). This vulnerability was exploited by the Equation Group tool ESTEEMAUDIT.

The other vulnerability published first by CNNVD was CVE-2017-8487. CNNVD published within one day, NVD published the next day (within two).

Among these Equation Group-related CVEs, NVD beat CNNVD to publication for 85 percent — much closer to its publication rate for Chinese APT associated CVEs (97 percent) than to the broad trend of 48 percent (NVD beats CNNVD to publication 52 percent of the time).

Outlook

It is always difficult to identify the hand of an intelligence service in an influence operation. In this research, we studied nearly 300 different CVEs that fell outside of the statistical norms in an attempt to identify undue influence upon the vulnerability reporting process in China. What we discovered were numerous clear examples of unexplainable behavior in vulnerability reporting by CNNVD, and cases where we believe the MSS likely have interfered to delay publication. We further revealed that CNNVD is essentially a shell; it has a website but appears to be separate from CNITSEC and the MSS in name only.

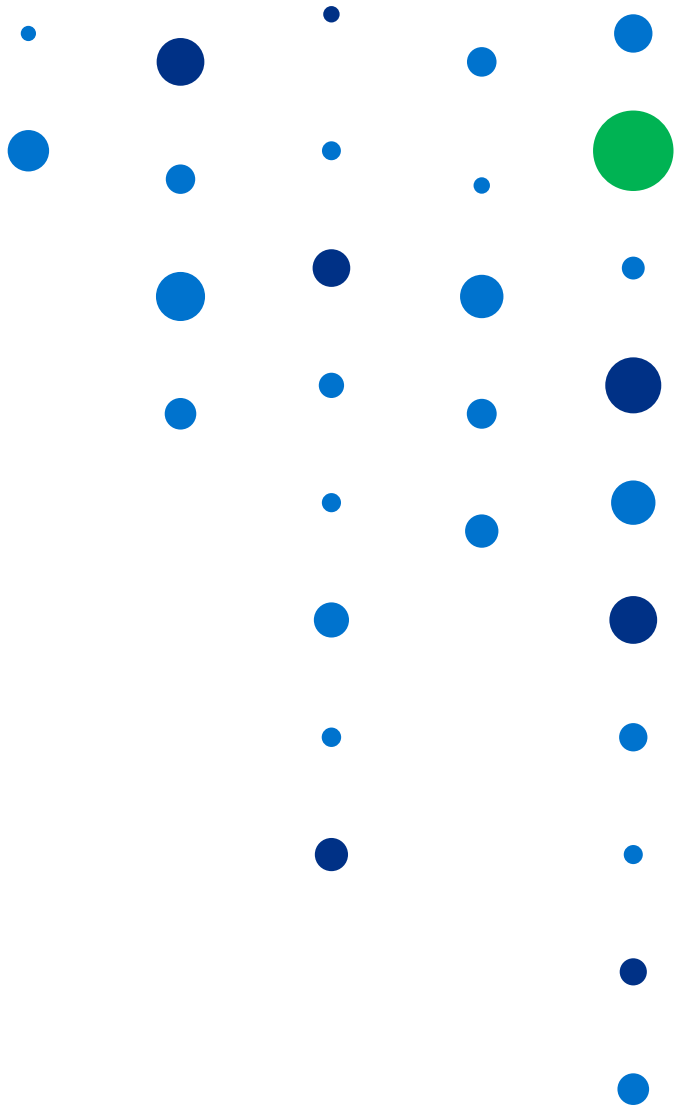
This data points to a larger conclusion, that China has a vulnerability evaluation process in which High-threat vulnerabilities are likely evaluated for their utility in intelligence operations before publication by CNNVD. Our analysis of these critical statistical deviations highlights why an intelligence service should not manage the vulnerability publication process — it is impossible for an intelligence service to equally uphold the mandates for both vulnerability reporting (transparency) and intelligence operations (secrecy). Our analysis of this dataset demonstrates that in China, one mandate is typically sacrificed — that of transparency.

When malicious cyber actors and security teams are racing to exploit or patch vulnerabilities, having access to the latest information is critical, but is only one part of the story. Speed is important, but content is as well.

Broadly, CNNVD is still faster to report vulnerabilities of all severities than NVD, however, the content of the publications can be inferior and there is likely interference by the MSS in delaying the publication of operationally useful CVEs. Companies and individual users should not rely on a single datasource for vulnerability reporting, no matter how quickly the source publishes. As our research has demonstrated, CNNVD is typically faster to publication than NVD, but NVD usually contains better content, references, and remediation information. Both databases are useful and have their own individual strengths and weaknesses and are valuable resources for vulnerability reporting.

Appendix A: CVE associated with Chinese state-sponsored cyber activity used in this study.

- CVE-2009-3957
- CVE-2009-4324
- CVE-2010-2861
- CVE-2010-2883
- CVE-2010-3333
- CVE-2010-3962
- CVE-2011-2462
- CVE-2011-3544
- CVE-2012-0158
- CVE-2012-4681
- CVE-2012-4792
- CVE-2013-0422
- CVE-2013-1347
- CVE-2013-2551
- CVE-2013-3893
- CVE-2013-3906
- CVE-2013-3918
- CVE-2014-0322
- CVE-2014-0502
- CVE-2014-1761
- CVE-2014-1776
- CVE-2014-6271
- CVE-2014-6332
- CVE-2014-9163
- CVE-2015-1641
- CVE-2015-2502
- CVE-2015-2545
- CVE-2015-3113
- CVE-2015-5122
- CVE-2016-0063
- CVE-2017-0199



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.