Recorded Future

CYBER THREAT ANALYSIS

China Altered Public Vulnerability Data to Conceal MSS Influence

By Priscilla Moriuchi and Dr. Bill Ladd
Recorded Future

CTA-2018-0309

Executive Summary

In November 2017, Recorded Future published research examining the publication speed for China's National Vulnerability Database (CNNVD). While conducting that research, we discovered that China had a process for evaluating whether high-threat vulnerabilities had operational utility in intelligence operations before publishing them to the CNNVD. In revisiting that analysis, we discovered that CNNVD had altered their initial vulnerability publication dates in what we assess is an attempt to cover up that evaluation process.

Key Judgments

- CNNVD altered the original publication dates in its public database for at least 267 vulnerabilities we identified as statistical outliers in our research published in November 2017.
- We assessed in November that CNNVD had a formal vulnerability evaluation process in which high-threat CVEs were evaluated for their operational utility by the MSS before publication, and that the publication lag was one way to identify vulnerabilities that the MSS was likely considering for use in offensive cyber operations. CNNVD's outright manipulation of these dates implicitly confirmed this assessment.
- By retroactively changing the original publication dates on these statistical outliers, CNNVD attempted to hide the evidence of this evaluation process, obfuscate which vulnerabilities the MSS may be utilizing, and limit the methods researchers can use to anticipate Chinese APT behavior.
- This large-scale manipulation of vulnerability data undermines trust in the CNNVD process and could compromise security operations relying solely on the CNNVD for that information.
- View the raw CNNVD data set here.

Background

In November 2017, we analyzed and compared the publication speeds of the U.S. National Vulnerability Database (NVD) and Chinese National Vulnerability Databases (CNNVD). At a high level, we established that CNNVD is faster than NVD in reporting vulnerabilities — NVD trails CNNVD in average time between initial disclosure and database inclusion (33 days versus 13 days).

We also discovered that CNNVD is essentially a shell for the Ministry of State Security (MSS); it has a website, but appears to be separate from the MSS in name only. This is important because the MSS is not just a foreign intelligence service, but it also has a large, and arguably more important, domestic intelligence mandate. Recognizing the importance of

the domestic mission is key to understanding why the MSS would manipulate data that is primarily consumed by Chinese or regional users.
Lastly, when we studied exceptions to this general pattern of CNNVD being quicker than NVD, we discovered evidence for CNNVD's vulnerability evaluation process — in which high-threat CVEs are likely evaluated for their operational utility by the MSS before publication.

Roughly six months after our initial reports, we decided to revisit the analysis to discern if earlier observed trends and patterns remained.

Threat Analysis

U.S. NVD — CNNVD Comparison

In our original report on NVD and CNNVD publication speeds, we observed that the average delay between a vulnerability being publicly disclosed on the web and being included in NVD was 33 days. Looking more broadly, we saw that it took 20 days to report on 75 percent of the disclosed vulnerabilities and 92 days to report on 90 percent.

In contrast, CNNVD averaged a 13-day delay and reached 75 percent disclosure by six days, and 90 percent by 18 days.

These analyses were based on a two-year window of disclosure data. We rolled the two-year window forward six months and saw that NVD had improved. The average was down to 27 days. Since three quarters of the data was the same, this suggests that the more recent data is being captured much more quickly. Similar improvements were seen in the time to reach 75 percent (15 days) and 90 percent (72 days).

When we looked at CNNVD, we saw essentially no change in the delays or reporting speed — they are still faster to publication than NVD.

We also saw that six months ago there were 1,746 CVEs reported in CNNVD that were not covered in NVD. This is because NVD relies upon voluntary submissions from vendors and CVE Numbering Authorities (CNAs) associated with the vulnerabilities, and uses MITRE's CVE Dictionary as its sole source. This was particularly frustrating as NVD is actually responsible (through MITRE) for managing the assignment of CVE identifiers.

Today there are 1,651 CVEs reported in CNNVD that are not covered in NVD. NVD is clearly getting faster, as well as working through the backlog of uncovered CVEs.

Data Manipulations in CNNVD

As we began to re-examine the data on CNNVD, and particularly the “outliers” — CVEs that 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 — we noticed that the publication date for the two vulnerabilities we highlighted in November had been altered. Specifically, the initial CNNVD publication dates for the two vulnerabilities had been backdated to match NVD and erase the publication lag.

Starting on the next page, find two sets of screenshots of the CNNVD entries — the first in each set from October 2017, and the second from February 2018.

CVE-2017-0199

Screenshot taken October 20, 2017 and published November 16, 2017. Publication date is listed as June 7, 2017.

Screenshot taken February 13, 2018. The original publication date has been changed from June 7, 2017 to April 13, 2017, a backdating of 56 days.

CVE-2016-10136

Screenshot taken October 23, 2017 and published November 16, 2017. Publication date is listed as September 6, 2017.

Screenshot taken February 13, 2018. The original publication date has been changed from September 6, 2017 to January 13, 2017, a backdating of 236 days.

Both sets of screenshots show that the original publication date for each CVE was altered sometime between October 24, 2017 and February 13, 2018 to reflect a date closer to NVD's publication date. For CVE-2017-0199, NVD published on April 12, 2017, and for CVE-2016-10136, NVD published on January 13, 2017.

After re-validating the publication date for each CVE, we identified as a statistical outlier, we discovered that 267 of the 268 CNNVD original publication dates had been altered since November 2017 with an average backdate of 57 days. Each date was changed post-publication to approximate or beat NVD's publication date. See this link for the complete data set.

Further, the publication dates for many outlier CVEs that were reported outside of our original date range (September 13, 2015 through September 13, 2017) but before our report was published (on November 16, 2017) were also altered in the same manner. We identified 75 new outlier vulnerabilities that were initially published between September 13 and November 16, 2017. Of those 75 CVEs, 72 vulnerabilities were backdated and the publication lags erased.

What Does This Mean?

We assessed in November that we discovered a formal vulnerability evaluation and obfuscation process at CNNVD in which high-threat CVEs are evaluated for their operational utility by the MSS before publication. This process meant that CNNVD would delay public notification, patching, and remediation guidance so the MSS could assess whether a vulnerability would be useful in their intelligence operations.

This systemic retroactive alteration of original publication dates by CNNVD is an attempt to hide the evidence of this process, obfuscate which vulnerabilities the MSS may be utilizing, and limit the methods researchers can use to anticipate Chinese APT behavior. There is no other logical explanation as to why only the initial publication dates for outlier CVEs would have been altered. While we did not query the publication dates of all 17,000+ CVEs listed in both NVD and CNNVD, we did query a portion of non-outlier CVEs and discovered no manipulation of publication dates.

Further, we did not publish all 268 CVE numbers which fell into the outlier category, nor were we able to anticipate which CVEs would become outliers after our original data sample (which ended on September 13, 2017). We were transparent with our methodology for identifying these outliers, and anyone with access to CNNVD data could replicate our results. We raise this because 267 out of the initial 268 vulnerability publication dates were manipulated, as well as 72 out of 75 outliers that we only identified when updating our research in mid-February.

99 percent of all outlier CVEs were altered to erase the publication lag.

In order to alter the original publication dates on all 343 of these CVEs, CNNVD needed to replicate our methodology for identifying outliers, apply it to their data set, and decide which date they would fraudulently claim to have originally published. Backdating the outlier CVE would prevent researchers from conducting an historical analysis of CNNVD trends and would conceal evidence of the MSS's operational evaluation program.

Despite CNNVD's manipulation of the initial publication dates, it is still possible to identify which vulnerabilities the MSS may be exploiting. Specific tracking queries and techniques have been shared with Recorded Future users.

Outlook

CNNVD's manipulation of its vulnerability publication data ultimately reveals more than it conceals. This is mainly a result of the Chinese state's all-encompassing desire for information control, whereupon it has allowed a public service organization with a transparency mandate to be run by an intelligence service with a secrecy mandate.

First, the selective backdating of vulnerability publication for the outliers is essentially a tacit confirmation from CNNVD of their vulnerability evaluation program and the operational use of some delayed vulnerabilities. Changing the dates after publication prevents researchers from conducting bulk historical analysis of CVE publication and from identifying vulnerabilities which the MSS or Chinese intelligence services may be exploiting in operations.

Second, while many think of the MSS as primarily a foreign intelligence service, it also has a large, and arguably more important, domestic intelligence mandate. Understanding this dynamic is key to understanding why the MSS would manipulate data that is primarily consumed by Asian or regional users. Many of the targets of operations that utilize exploits for delayed publication vulnerabilities would likely be against domestic or regional intelligence priorities. Delayed publication could also be operationally useful because it could allow the MSS to monitor the rates of international patching or remediation measures, which could also be a factor in deciding whether or not to deploy an exploit in foreign space.

Third, from a public service and transparency perspective, there could be larger liability issues for companies and institutions that rely solely on CNNVD data. If a company is victimized by an exploit for a vulnerability during the altered period of time, unless it kept a historical record of all CNNVD initial report dates, it could face questions about why it did not remediate a vulnerability that it did not know about.

For example, if a company was victimized by an exploit for CVE-2017-0199 on May 15, 2017 and used CNNVD data, then it would not have known to remediate that vulnerability until June 7, 2017. Since CNNVD altered the publication date for this vulnerability after publication to April 13, 2017, a current examination of the vulnerability could lead investigators to conclude that the company was aware of the vulnerability after April 13 but chose not to remediate. Depending upon the data loss, the breach, and the country, this data manipulation could put companies at further risk for fines or legal action resulting from an intrusion.

China's recently instituted Cybersecurity Law (CSL) mandates that companies operating in China adopt a "tiered system of network security protections" and can hold companies both legally and financially responsible for a "network security incident." However, for a foreign multinational company to comply with all the provisions of the CSL means that it may at the same time be violating Western laws or regulations against cooperating with Chinese security and intelligence services.

Lastly, this data manipulation reinforces the dominance of the secrecy mandate over transparency in China. Instead of taking steps to remove the undue influence of secrecy and the intelligence services over vulnerability reporting, CNNVD has gone the opposite way and sought instead to further conceal that influence. This problem of MSS influence in China's information security architecture is one we have followed for some time, and will continue to research.