Prioritizing “critical” vulnerabilities: A threat intelligence perspective

intel471.com/blog/prioritizing-critical-vulnerabilities-a-threat-intelligence-perspective

By the Intel 471 Intelligence Analysis team.

Recently, there have been many vendor security advisories containing multiple critical vulnerabilities potentially impacting organizations that may be conflicted with patch prioritization when looking at the variables seen for each reported vulnerability. Threat intelligence can supplement publicly disclosed information and provide a contextual view of exploitation efforts and general interest in open source reported vulnerabilities from an underground threat actor perspective. For instance, our vulnerability intelligence product uses information disclosed by vendor advisories, open source repositories and research companies’ analyses to determine a certain level of risk, but we also take into consideration the scope of underground activity that can be seen surrounding critical vulnerability announcements. It is important to note that our risk assessment is assigned as a probability of current, active exploitation versus organization-specific risk.

Over the course of a year, we observed consistency across underground activity responding to critical vulnerability disclosures and leading up to exploit development. These indicators could further help identify potential elevation of risk to your organization by recognizing events such as spikes of activity that commonly occur prior to successful exploitation attempts. This is far from a one-size-fits-all approach and won’t necessarily give you an easy-to-prioritize list, but through the examples shown below, you will see this theory applied to recent critical vulnerabilities overlaid with threat actor activity observed over time.

Disclosure to exploitation

After the initial open source disclosure of a critical vulnerability that reportedly received the highest severity rating available, a pattern of activity can be observed in the underground. There is an initial surge in posts made by threat actors who copy and paste information directly from open source reports. Additionally, there are several forum threads started where threat actors discuss the possibility of exploitation or seek partners to assist in the development of proof of concept (PoC) and exploit code that leverage the newly announced vulnerability. Closely following these discussions, several threat actors will advertise claims of PoCs and exploits that have successfully been developed, however, claims within this timeframe are typically false.

After this initial deluge of information, activity surrounding mentions of the vulnerability slows and there are fewer observed reposts of open source information. Paired with this, a few threat actors may advertise high dollar PoCs or exploits in a limited supply. For example, an actor will claim to have an exploit for a recently disclosed critical vulnerability, including

the common vulnerabilities and exposures (CVE) ID or its alias in the initial post. The privately developed code will be priced around US $1,000 to US $4,000 and the actor will state only a few copies are available for purchase. It is common to see this activity reported as alleged code development as they would need to be purchased or verified by a reliable secondary source to report them as a source of truth. Vendors and vulnerability researchers likely would include information of existing credible exploit development and successful exploitation of a vulnerability. These sources also may expedite the development of exploits, such as when you see a successful PoC released after patching information for impacted products is provided by the vendor.

Once threat actors share advertisements of code development, publicly available PoCs are not far behind, if not already released. If you are not immediately aware of publicly available code, conversations on the pricey exploit advertisement threads will point to it. Threat actors will share links to open source PoCs or exploits in response to the initial sales post and will leave comments such as “this is a rip off,” “it must be fake, you can get this for free” and more. Notably, successful exploit development does not necessarily indicate all interested financially motivated cybercriminals will leverage the vulnerability for attacks. While there might be an increase in exploitation attempts, many threat actors will lack the sophistication required to take their interest to the next level.

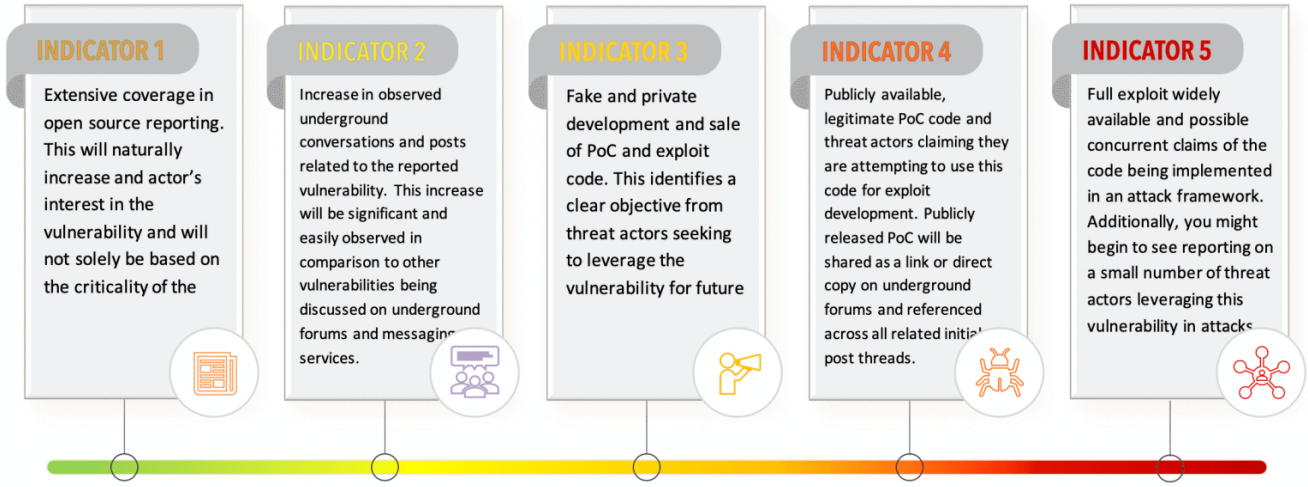
As the disclosure to exploit cycle ends, reporting on threat actors successfully leveraging the vulnerability in attack techniques and procedures may be delayed. Attackers can be cautious and use nonspecific details if they report initial entry methods at all, such as claiming to leverage a type of vulnerability or only providing the name of the vulnerable system. Evidence of this activity allows us to identify threat actors that claim to leverage a specific vulnerability to carry out consistently intrusive cybercriminal activity.

Priority indicators to assess risk of exploitation

The threat intelligence variables that add contextual risk to critical vulnerability prioritization can be cumbersome if your organization is affected by many recent advisories. In essence, you would be trying to monitor trends for 20 or more high severity vulnerabilities. The observations presented above can be summarized into five indicators that should trigger an increase in priority ranking.

1. Indicator one – Extensive coverage in open source reporting. This will naturally increase an actor’s interest in the vulnerability and will not solely be based on the criticality of the reported CVE.
2. Indicator two – Increase in observed underground conversations and posts related to the reported vulnerability. This increase will be significant and easily observed in comparison to other vulnerabilities being discussed on underground forums and messaging services.

3. Indicator three – Fake and private development and sale of PoC and exploit code. This identifies a clear objective from threat actors seeking to leverage the vulnerability for future attacks.
4. Indicator four – Publicly available, legitimate PoC code and threat actors claiming they are attempting to use this code for exploit development. Publicly released PoC code will be shared as a link or direct copy-paste on underground forums and referenced across all related initial post threads.
5. Indicator five – Full exploit widely available and possibly concurrent claims of the code being implemented in an attack framework. Additionally, you might begin to see reporting on a small number of threat actors leveraging this vulnerability in attacks.



Theory into practice

Using the indicators above, you can begin to map these trends across current critical vulnerabilities. Below you will see three critical vulnerabilities reviewed against this patterned activity including a timeline of underground activity and risk score.

CVE-2019-19781

This Citrix Application Delivery Controller, Citrix Gateway and Citrix SD-WAN WANOP appliance vulnerability, CVE-2019-19781, was disclosed in December 2019 and last updated in the U.S. National Vulnerability Database (NVD) in January 2020. In December 2019, we began to see less sophisticated threat actors share information from open source reports about CVE-2019-19781 and new forum threads started where actors sought to buy an exploit for the vulnerability. Discussions about the potential exploitation of the vulnerability continued until a publicly available exploit was observed in January 2020 and subsequently shared in the underground. Several exploit variants were circulated by threat actors commonly known for sharing publicly available PoC and exploit code.

This vulnerability continues to be high risk to organizations with unpatched affected Citrix systems. We reported on threat actors who claimed this vulnerability allowed them access into vulnerable systems as they attempted to move laterally through impacted networks. The overall risk of exploitation score is high.

December 2019

- Several actors across multiple popular cybercrime forums posted information from open source reporting about the disclosure of CVE-2019-19781.
- A long-standing member of the Russian-language underground community started a post thread where the actor advertised funds available to purchase an exploit for the Citrix vulnerability. Several actors replied expressing a similar interest or discussing exploitability of CVE-2019-19781.
- A prolific seller of network access possibly leveraged the vulnerability to gain unauthorized network access to several organizations. The assessment was not confirmed but the timing of the disclosure and advertised accesses were concurrent.

January 2020

- An exploit for the Citrix vulnerability was publicly available. An actor posted the GitHub link on a previously opened post thread and several actors circulated exploits for the vulnerability.
- An actor shared several code variants for CVE-2019-19781. This actor commonly shares copied PoC and exploit code from open sources including Exploit DB, Packet Storm and GitHub.

February 2020

A Russian-speaking actor was suspected to have leveraged the Citrix vulnerability after released compromised access revealed the impacted company uses Citrix System Software, however, the assessment was not confirmed.

May 2020

A relatively new actor allegedly leveraged CVE-2019-19781 to sell compromised network accesses on underground forums. The actor claimed to use publicly available code for exploitation after scanning the internet for vulnerable hosts.

June 2020

A handful of actors, including a notable threat actor with a positive underground reputation, claimed responsibility for many compromised network accesses likely using the Citrix vulnerability as an initial attack vector into compromised victim organizations.

CVE-2020-5902

The F5 Traffic Management User Interface (TMUI), also referred to as the Configuration utility, reportedly had an RCE vulnerability in multiple versions of BIG-IP that was disclosed publicly as CVE-2020-5902 June 30, 2020. This vulnerability quickly cycled through the priority indicators of underground activity, which added to the vulnerability's criticality and overall risk of possible exploitation. The vendor reported the vulnerability with a Common Vulnerability Scoring System (CVSS) of 10.0, the highest score a CVE can receive. The F5 vulnerability allowed unauthenticated attackers or authenticated users with network access to execute arbitrary system commands, create or delete files, disable services and execute arbitrary Java code. Although the vendor released fixed versions and mitigation information, there was rapid development of exploit code and implementation into an attack framework.

Following common trends, several actors shared information from multiple open source reports that discussed the vulnerability, an actor shared an alleged nmap exploit for CVE-2020-5902. Once a Metasploit module was observed publicly, an actor known for copying code from open sources shared it on an underground forum. Because the vulnerability was quickly productized and there was evidence of threat actors attempting to leverage the CVE in attacks, the overall risk of exploitation score is high.

July 2020

- Several actors posted information from open source reporting about the disclosure of CVE-2020-5902.
  An actor posted an alleged nmap exploit for the F5 BIG-IP vulnerability stating: "Here I'm posting nmap script to exploit it. I am loving this vulnerability."
- A notable Turkish-speaking actor shared an exploit and Metasploit module for CVE-2020-5902. The actor commonly shares PoC and exploit code available in open sources including Exploit DB, GitHub and Packet Storm.

CVE-2020-1350

The Microsoft Windows domain name system (DNS) servers remote code execution (RCE) vulnerability, CVE-2020-1350, was disclosed in July 2020 and is still cycling through the initial priority indicators of observed underground activity. There was an extensive amount of open source coverage of this vulnerability, which referenced risk scoring previously assigned to the BlueKeep vulnerability CVE-2019-0708. The criticality of the vulnerability, impacted vendor, type of vulnerability and widespread reporting of CVE-2020-1350 were indicators of its severity. Following the outlined behavior, after the disclosure of the vulnerability and released patching information, we observed a near-immediate increase in underground mentions of this vulnerability including rick-rolling PoCs repeatedly shared.

There is clear underground interest in CVE-2020-1350 based on threat actor posts seeking to develop code to leverage this vulnerability. However, a closer look at the actors that expressed an initial interest in leveraging the vulnerability shows no specific historical activity to indicate these individuals are sophisticated enough to carry out an exploitation of

the SIGRed vulnerability alone. The activity remains an indicator of increase in risk scoring and probability of exploitation, but there likely will be many follow-on indicators that will press the severity higher. The current overall risk of exploitation score is medium.

July 2020

- Several threat actors posted information from open source reporting about CVE-2020-1350 and evidence of publicly available imitation PoC code was observed.
- A relatively new actor started a post thread in a popular English-language cybercrime forum expressing interest in exploring the vulnerability and potentially building something with it, but there was no observed interest in the actor's post. The actor previously advertised dumped databases obtained by exploiting enterprise resource planning software.
- A denial of service (DoS) PoC was released publicly on GitHub.

Wrap up

Understanding the phases of underground activity driven by critical vulnerability disclosures can contextualize new and existing high-impact CVEs. The five indicators provided above were established based on general trend analysis as a point of reference to assist in developing a priority assessment for critical CVEs.