Vulnerability management: user guide

Positive Technologies

ptsecurity.com

Contents

Introduction

Digitalization and the transition to remote work have led to an increase in the number of attacks exploiting vulnerabilities. Every quarter we see the emergence of new high-profile vulnerabilities that attackers immediately weaponize, such as ProxyLogon, vulnerabilities in Accellion FTA, Zerologon, and Log4Shell. By exploiting vulnerabilities, cybercriminals can not only penetrate a company's network, but also actuate unacceptable events. A notorious example is the attack against logistics services provider Bakker Logistiek in April. The attackers managed to disrupt the company's internal business processes and delivery operations. They exploited Microsoft Exchange ProxyLogon vulnerabilities, which allowed them to distribute ransomware. The consequences were dire; for example, supermarket chain Albert Heijn reported a shortage of certain food products.

In order to prevent unacceptable events, companies must eliminate potential attack vectors by which attackers can reach target systems. This also includes elimination of vulnerabilities. Detection of vulnerabilities and timely installation of security updates must be an integral part of the vulnerability management process. Some companies implement vulnerability management in order to meet regulatory requirements, while others use it to reach the next level of information security maturity. However, our surveys show that such companies are just a drop in the ocean.

We analyzed data obtained during the MaxPatrol VM pilot projects in 2021, in which we scanned over 15,000 hosts in government, scientific, educational, financial, and telecom companies. For our research, we selected only those projects whose scope was sufficient to obtain objective results. In addition, we aggregated the information on vulnerabilities found during the penetration testing projects in 2020–2021. We will outline the results of our analysis, describe the problems related to the vulnerability management process, and share recommendations for optimizing this process.

Interesting fact

Trend Micro researchers demonstrated that the average organization takes between 60 to 150 days to fix a vulnerability

Trending vulnerabilities

In each pilot project, we discovered an average of 31,066 vulnerabilities. The severity of these vulnerabilities was assessed according to the Common Vulnerability Scoring System (CVSS) version 3.1. Critical vulnerabilities were found in all pilot projects.

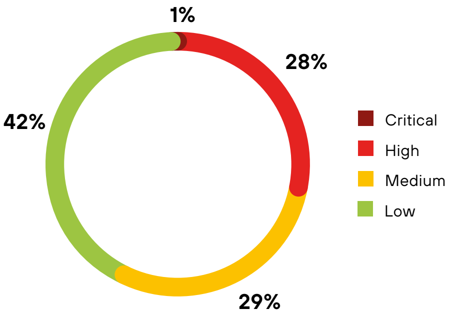


Figure 1. Vulnerabilities detected during pilot projects, by level of severity

Some vulnerabilities are exploited by criminals more often than others. This is especially true for recently published dangerous vulnerabilities, for which most organizations have not yet installed security updates. We call such vulnerabilities trending. If these vulnerabilities are detected in your infrastructure, you should pay special attention to them: they are easily integrated into the attack chain, and for some of them a public exploit is available (or will soon be).The average number of trending vulnerabilities per pilot project is 861 (3% of all vulnerabilities found during the project).

Trending vulnerabilities are dangerous vulnerabilities that are widely used in attacks or are likely to be used in the near future.

Examples of trending vulnerabilities

Vulnerability type	Target	Vulnerability identifier	CVSS score
Remote code execution	Windows DNS server	CVE-2020-1350	10.0
Privilege escalation (Zerologon)	Netlogon	CVE-2020-1472	10.0
Remote code execution (BlueKeep)	RDP	CVE-2019-0708	9.8
Remote code execution	Internet Information Services (IIS)	CVE-2021-31166	9.8
Remote code execution	Apache Tomcat AJP	CVE-2020-1938	9.8
Bypassing authentication	libc in OpenBSD 6.6	CVE-2019-19521	9.8
Remote code execution	MSHTML engine	CVE-2019-0541	8.8
Remote code execution (Bad Neighbor)	Windows TCP/IP	CVE-2020-16898	8.8
Remote code execution (PrintNightmare)	Windows Print Spooler Service	CVE-2021-34527	8.8
Escalation of privileges	Windows Print Spooler Service	CVE-2021-1675	8.8
Remote code execution (MS17-010)	SMBv1	CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148	8.1
Data spoofing	Windows CryptoAPI	CVE-2020-0601	8.1
Remote code execution (ProxyLogon)	Microsoft Exchange Server	CVE-2021-26855	9.8
		CVE-2021-27065	7.8
Escalation of privileges	Windows Win32k	CVE-2021-1732	7.8
Escalation of privileges	Windows Kernel	CVE-2020-17087	7.8

On average, no more than three percent of vulnerabilities in a company's infrastructure are truly critical and require priority action for remediation; at the same time, they may not have the highest CVSS scores.

New trending vulnerabilities emerge regularly: for example, while we were preparing this research, a remote code execution vulnerability was detected in the Apache Log4j library (CVE-2021-44228). Criminals immediately took it in hand. If you are using this library, please read the Apache's security advisory.

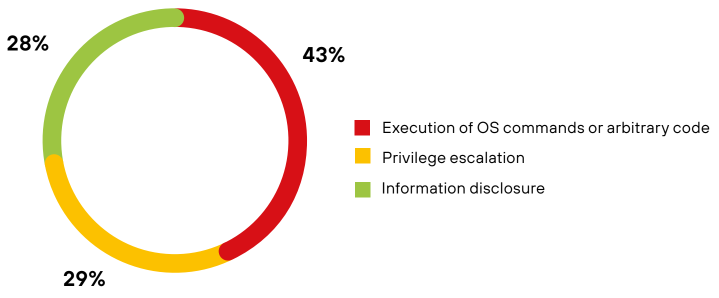


Figure 2. Result of exploitation of vulnerabilities in penetration tests (percentage of vulnerabilities)

If the vulnerability is successfully exploited, attackers can gain access to company resources and obtain the necessary privileges or information that will allow them to develop the attack. During penetration tests conducted in the second half of 2020 and the first half of 2021, software vulnerabilities were exploited in 41 projects. In most cases, our specialists exploited vulnerabilities to execute commands or arbitrary code.

If exploited, vulnerabilities let attackers trigger unwanted or even unacceptable events. Further in this research, we will look at possible consequences of vulnerabilities exploitation.

- **Access to the internal network**

In 60 percent of external security assessments, exploitation of known vulnerabilities in software enabled our experts to penetrate the corporate network. An example is the Microsoft Exchange Server remote code execution vulnerability CVE-2021-27065.

APT groups, in particular, HAFNIUM, use the ProxyLogon vulnerabilities CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, and CVE-2021-26855 in their mining and ransomware campaigns. In one week, HAFNIUM attacked at least 30,000 organizations in the U.S. and hundreds of thousands of companies around the world. The purpose of this malicious campaign was to gain access to the IT infrastructure of companies and steal sensitive information.

A key system is an information system that an intruder needs to compromise in order to develop an attack on a target system, or a system whose compromise would greatly simplify the scenario for attacking target systems.

A target system is an information system whose compromise can lead directly to an unacceptable event for the business.

- **Access to key and target systems**

A vulnerability in Windows Print Spooler (CVE-2021-1675) discovered during penetration tests in local networks of several companies allowed our experts to gain maximum privileges in domains. The Vice Society and Magniber ransomware operators used this vulnerability in combination with CVE-2021-34527 to deliver their malware.

The CVE-2020-1472 (Zerologon) vulnerability was exploited in penetration tests at 28 percent of companies, and in most cases our experts obtained access to the domain controller with maximum privileges. Zerologon was widely exploited by criminals spreading the Ryuk malware and the Trickbot Trojan. During our pilot projects, Zerologon was encountered in two campaigns.

The CVE-2021-1732 vulnerability used to escalate privileges in the system, combined with other vulnerabilities in browsers, can be used to bypass sandbox checks. This vulnerability is widely exploited by the BITTER APT cyberespionage group (APT-C-08). Incidentally, CVE-2021-1732 was detected in 29 percent of the companies that participated in MaxPatrol VM pilot projects.

Surprisingly, the infamous EternalBlue vulnerability that made headlines in 2017 is still relevant today. By exploiting this vulnerability, attackers spread the WannaCry ransomware at a rate of 10,000 devices per hour, infecting more than 230,000 Windows computers in 150 countries in one day. Many companies were affected, including Britain's National Health Service, which had to cancel thousands of appointments and operations. In penetration tests conducted in 2020–2021, vulnerabilities from the Microsoft Security Bulletin MS17-010 were found on the LAN of 18 percent of companies.

As opposed to a real attack, in penetration testing, some vulnerabilities can only be checked in a test environment, for example, CVE-2017-6868 in the Siemens SIMATIC CP 44x-1 module, which allows executing commands on a programmable logic controller. If exploited at a real critical infrastructure facility, this vulnerability would lead to a disruption of its operations or even an accident.

Do all vulnerabilities need to be fixed?

Imagine reading a pilot report: we have scanned your infrastructure and detected 31,066 vulnerabilities. The first thing that comes to mind when reading this is that you cannot fix such a great number of vulnerabilities quickly. In this case, which ones should be fixed first?

First, let's answer the question of why you should not rely only on CVSS score or prioritize vulnerabilities based on this score. In our pilot projects, 29 percent of detected vulnerabilities were of critical or high severity. It would take a long time to eliminate that many vulnerabilities, but there is no guarantee that attackers would use those particular vulnerabilities to actuate an unacceptable event. Security assessments also proved that not all of the detected vulnerabilities can be used to develop an attack vector aimed at obtaining access to critical resources.

Not every vulnerability, even if it has a high CVSS score, can lead to the actuation of an unacceptable event for the company.

We identify two groups of factors that must be taken into account when prioritizing the elimination of vulnerabilities:

- The significance of the asset on which the vulnerability was detected and its accessibility to attackers. By significance we mean the consequences of exploiting a vulnerability, that is, what happens if attackers exploit a particular vulnerability on a specific asset; by accessibility we mean privileges attackers need to exploit the vulnerability.
- The severity of the vulnerability, the odds that it will be exploited, and whether the vulnerability is trending

An **asset** is an information system or a host valuable for an organization and that must be protected from cyberthreats.

Security professionals often forget about the first group of factors and focus instead on the second group.

Fewer than half of the questioned information security experts prioritize detected vulnerabilities based on the significance of assets on which they were found.

How to assess the importance of an asset? To evaluate an asset, the company's specialists, including top management, must first prepare a list of business-unacceptable events. Only then can they identify target and key systems and determine crucial assets. At the beginning of each pilot project, the company's specialists had to rank the assets in the test area by their importance. On average, there were 1,216 assets per project, of which only three percent were of high importance. These assets accounted for approximately six percent of all detected vulnerabilities.

42 is the average number of trending vulnerabilities on all highly important assets in a single project

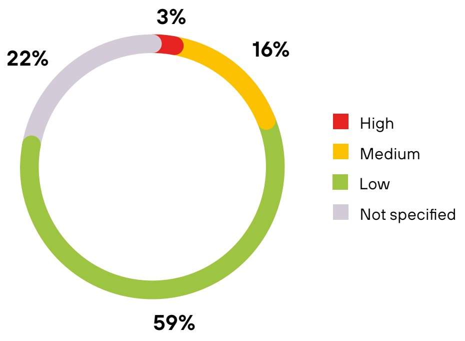


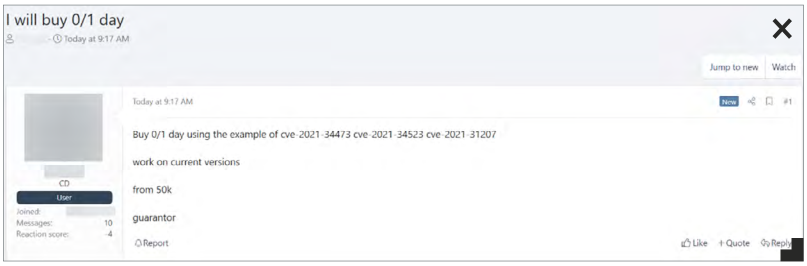
Figure 3. Importance of assets in pilot projects

An **asset of high importance** is the most significant information system or host that is part of key or target systems. Access to these systems can lead to the actuation of unacceptable events.

Another important parameter for an attacker is the availability of a host (asset) on which a vulnerability was discovered. In this case, you determine whether external attackers can exploit the vulnerability and which privileges they need to do so. For example, vulnerabilities that require an attacker to penetrate the LAN in order to exploit them will have a lower priority.

The second group of factors includes two parameters: CVSS score and availability of a public exploit, proof of concept (PoC), or Metasploit module. In addition to these parameters, we also recommend that companies consult our list of trending vulnerabilities and take into account whether a vulnerability is included in this list when prioritizing.

How important is it to take into account the availability of a publicly available exploit when prioritizing vulnerabilities? As soon as a public exploit for a vulnerability becomes available, cybercriminals pounce on it: sometimes they need just a few hours to exploit a fresh vulnerability. If attackers have sufficient knowledge about the infrastructure and the vulnerability, and have programming skills, they can write an exploit themselves. However, even if their skills are not enough or they do not want to develop the exploit, they can buy a ready-made exploit on a dark web forum.



I will buy 0/1 day

[redacted] · Today at 9:17 AM

Today at 9:17 AM

Buy 0/1 day using the example of cve-2021-34473 cve-2021-34523 cve-2021-31207

work on current versions

from 50k

guarantor

[redacted]
CD
User
Joined: [redacted]
Messages: 10
Reaction score: -4

Figure 4. Advertisement selling an exploit

According to our data, there was a public exploit for 81 percent of vulnerabilities used by attackers from Q1 2020 through Q4 2021. However, the lack of a public exploit does not guarantee that attackers will not write an exploit themselves or purchase it on a dark web forum.

In some cases, in order to exploit a vulnerability, attackers only needed a description of how to exploit it. On August 3, 2021, Tenable reported a vulnerability in Arcadyan routers that could let attackers bypass authentication (CVE-2021-20090). Three days later, Juniper Networks discovered that this vulnerability was used in several attack scenarios; for example, attackers tried to add vulnerable devices to the Mirai botnet.

A final question remains: in what sequence should the vulnerabilities be prioritized in order to then eliminate them?

Difficulty prioritizing

Before starting the prioritization, make sure that your hosts are scanned correctly. The vulnerability management process must cover the entire IT infrastructure of the company. Therefore, it is vital to check that all assets are identified, and make sure that if new hosts appear or some systems are disabled, the list of hosts to be scanned is timely updated. Otherwise, an important asset, such as a 1C server or a domain controller, may not be scanned.

It is vital that your security assessment system obtains information about the IT infrastructure not only through active scanning, but also from other systems (external directories or other information security solutions).

We recommend that you start the prioritization of vulnerabilities by assessing your assets. This approach will let you identify important assets and focus on protecting them first. This approach makes sense if you want to build an efficient security system.

Results-oriented security is a qualitatively and quantitatively measurable information security system that protects important assets and prevents unacceptable events.

1. To begin with, we suggest that you identify which events may cause unacceptable damage to your company, determine key and target systems, and rank the assets in terms of importance. At this stage, the main question is: what role does the asset play in your company's infrastructure? After all, the first thing to do is to protect the infrastructure penetration points as well as key and target systems.

2. Assess the potential impact of vulnerability exploitation. You need to understand what attackers will be able to do if they manage to exploit a vulnerability:

   - Actuate an unacceptable event?
   - Obtain access to a key system?
   - Obtain maximum privileges on the host?
   - Penetrate the company's internal network?

3. Next, we recommend that you rank the vulnerabilities by the availability of a public exploit or a PoC.

If the detected vulnerability is used in real attacks, that is a good reason to raise its priority or even eliminate it first, even if it requires deviation from the established prioritization process.

4. Assess the availability of the system for attackers and determine which privileges criminals need to exploit the vulnerability. At this stage, the main questions are: who has access to the system in which the vulnerability was found? Can this vulnerability be exploited by an external attacker?

   If a vulnerability is detected in a system located on the company's network perimeter, it can be easily reached and exploited by attackers.

5. Finally, determine the CVSS score of the vulnerability.

   This approach will help you fix the most dangerous vulnerabilities on truly important assets first. Only when the most important systems are protected, can we address vulnerabilities on less important assets, using the same principle.

   The described approach allows us to switch from the conventional vulnerability management process to truly efficient cybersecurity methods, the main goal being to protect the business from irreversible negative consequences. To make the vulnerability management process as efficient as possible, we recommend using modern automated systems, which not only perform asset inventory and detect vulnerabilities, but also help to build a clear and transparent interaction between the IT and the information security departments.

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com

For 20 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com