# Making the universe a safer place:

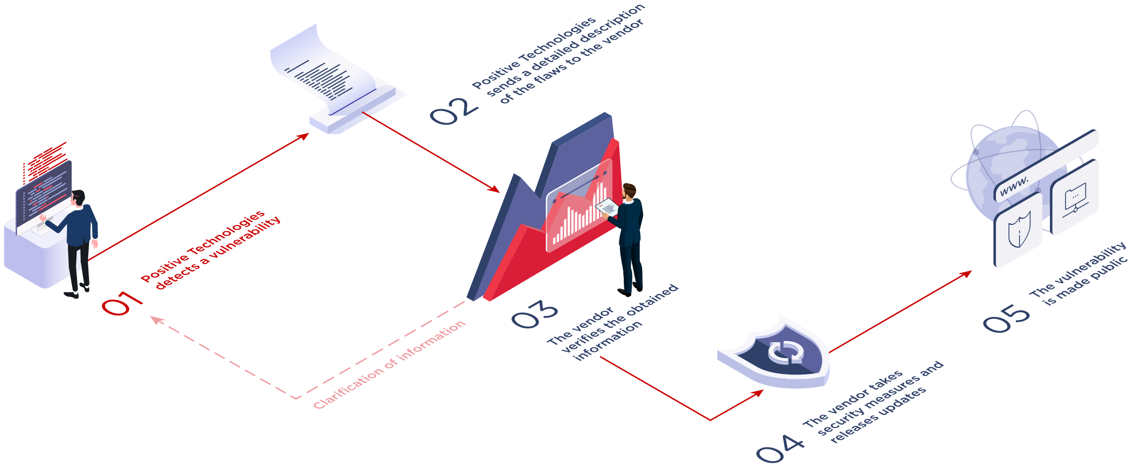
## Positive Technologies detects vulnerabilities

ptsecurity.com

"Software has bugs. This is normal," wrote David Heinemeier Hansson, developer of the Ruby on Rails programming language. However, if these bugs are not fixed, it can lead to serious financial consequences and even human losses. For example, at London's Heathrow airport, 42,000 bags were lost and 500 flights were canceled during the first 10 days after the opening of a new terminal due to flaws in the baggage handling system. In half an hour, US broker Knight Capital Group lost $440 million (almost the firm's entire capital) on the stock market because of insufficiently tested new trading software. Other such examples abound.

Detection and elimination of vulnerabilities is a joint task of software developers and information security experts. Positive Technologies contributes to this process by regularly informing software vendors of new vulnerabilities. Our company adheres to the principles of responsible disclosure. All of the vulnerabilities found are made known to the software manufacturers, including details of exploitation and recommendations on how to improve security. Only by agreement with the vendor and only after the vendor has fixed the bug and released an official security statement do we publish the results of our studies online. By detecting vulnerabilities, we improve cybersecurity around the world. If experts stop informing vendors of their mistakes and helping them to eliminate these flaws, cybercriminals will pounce. This is unacceptable.

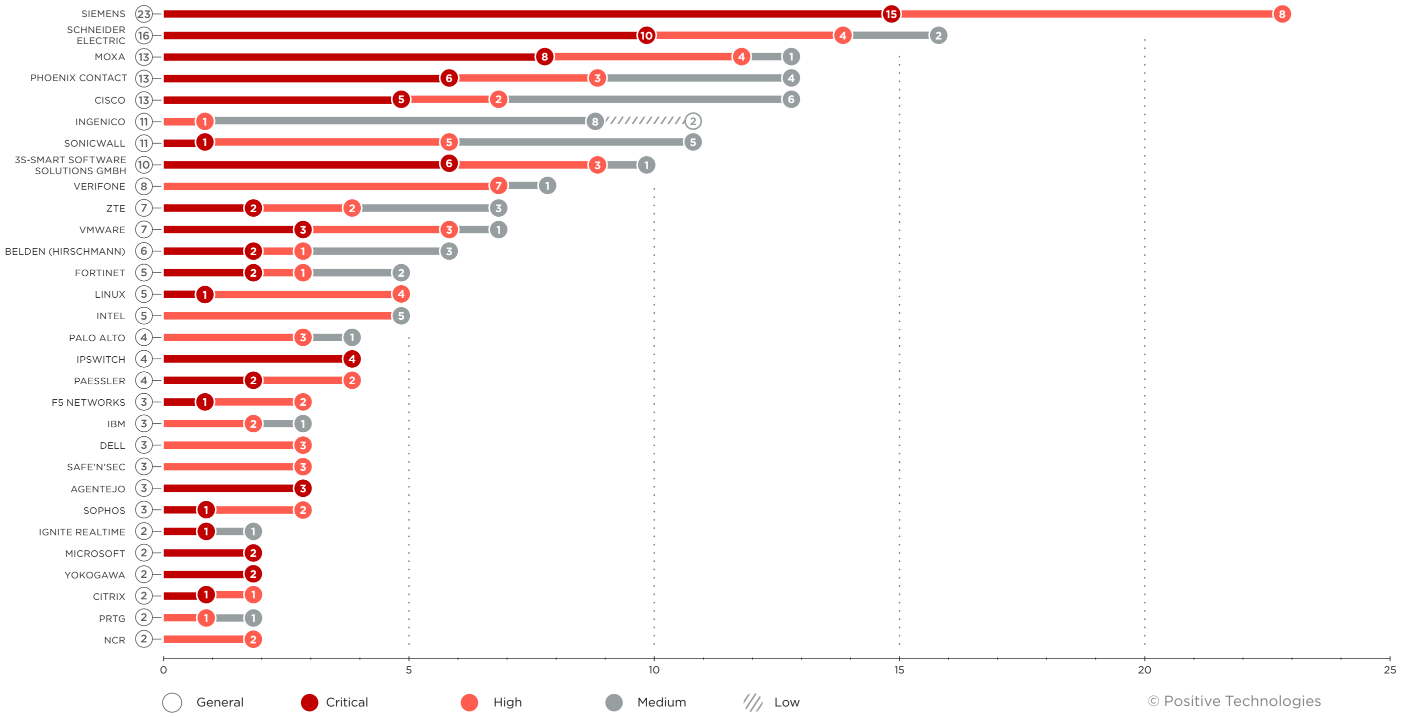
**Main scenario of interaction**
**with a vendor after detection of a vulnerability by Positive Technologies**


01 Positive Technologies detects a vulnerability
02 Positive Technologies sends a detailed description of the flaws to the vendor
03 The vendor verifies the obtained information
Clarification of information
04 The vendor takes security measures and releases updates
05 The vulnerability is made public
www.

## Results of three years of work

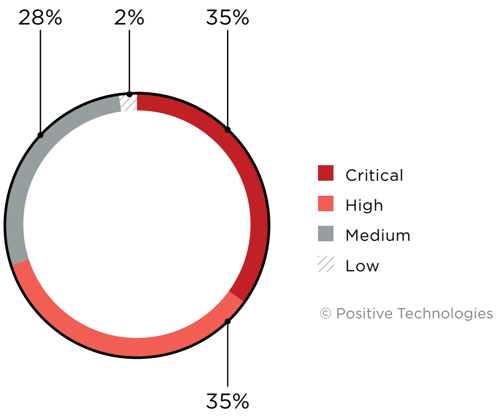
From 2018 to 2021, Positive Technologies detected over 250 vulnerabilities in software of 60 manufacturers, including Cisco, Citrix, IBM, Ingenico, Intel, Fortinet, Palo Alto, Microsoft, VMware, Hirschmann, Moxa, NCR, Schneider Electric, Siemens, Verifone and Yokogawa. 27 other vulnerabilities are still awaiting vendor confirmation.

Over the last three years, the highest number of dangerous vulnerabilities were found in hardware and software of the following manufacturers:



© Positive Technologies

Top 30 vendors by number and severity level of vulnerabilities detected by Positive Technologies over the last three years



© Positive Technologies

Severity level of detected vulnerabilities

70 percent of detected vulnerabilities were of high or critical severity, based on the Common Vulnerability Scoring System (CVSS 3.0). Critical vulnerabilities were found in hardware and software products of 23 vendors.

However, severity level of a vulnerability is not the only criterion of the importance of the work done. Software in which our experts detect vulnerabilities forms the backbone of the infrastructures of major companies across the world. These companies are leaders in their sectors. Any vulnerability in a crucial product instantly poses a threat to millions of companies. Below are just a few examples that demonstrate the extent of the problem.

## VPN access for hackers

In 2020, Positive Technologies detected and helped to eliminate two dangerous vulnerabilities in Cisco ASA firewall. At the time this research was published, over 220,000 devices were accessible from the Internet, and hackers could potentially exploit flaws in these devices. By using the first vulnerability, an external attacker could perform a DoS attack on vulnerable devices and disable the VPN. In other words, deprive companies of remote working. Now that many companies have continued to operate remotely, this problem can seriously affect business processes. In addition, a VPN is often used to connect various segments of the corporate network, which means that key systems may also be affected, such as ERP or corporate mail. The second vulnerability allowed hackers to read a cookie of a VPN-connected user from the memory of an affected device, specify the stolen identifier in Cisco VPN Client, and access the target company's internal network. As a result, the company could have been compromised remotely.

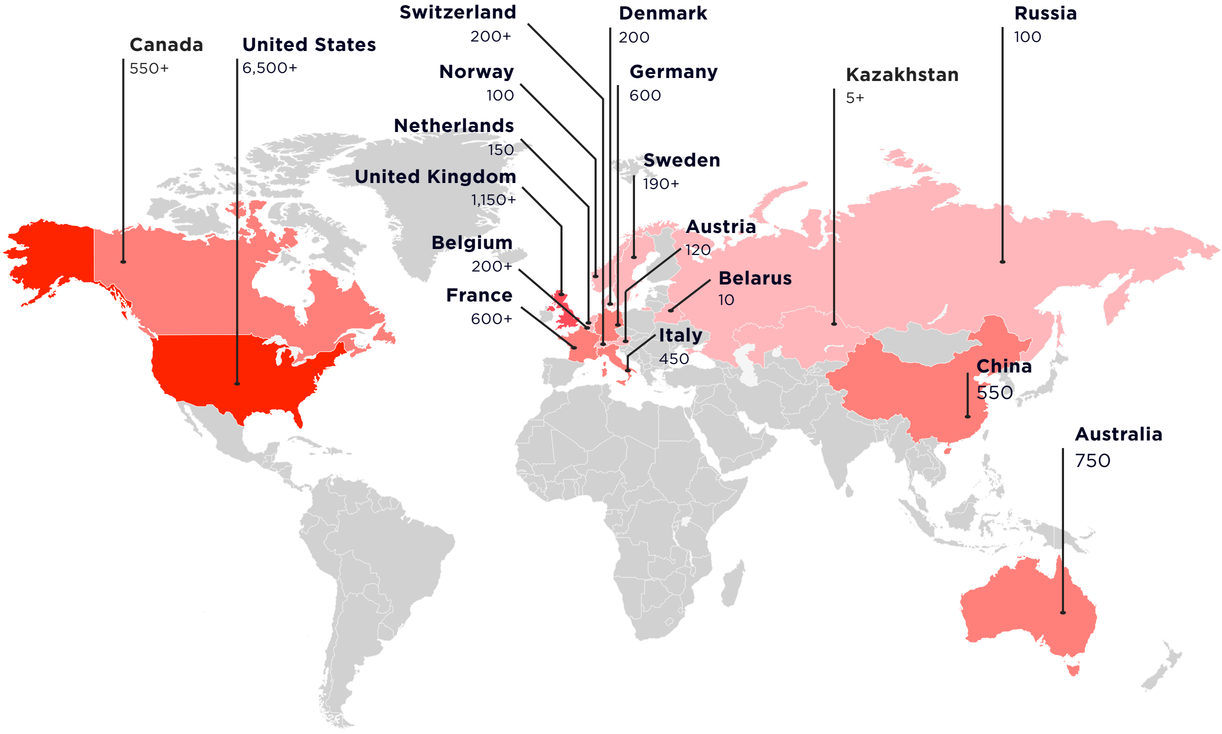
Vulnerabilities are often found in solutions designed for protection. For example, our experts helped to fix vulnerabilities in software of the following leading manufacturers:

- SonicWall firewalls (The company ranks fifth among manufacturers of hardware tools worldwide.)
- Rapid7 vulnerability management system (The company is a leading manufacturer of analytics and security automation tools.)
- PAN-OS operating system used by Palo Alto Networks next-generation firewalls (NGFW) (Palo Alto Networks is one of the leaders in information security.)
- FortiWeb firewalls for web applications by Fortinet (The company ranks first by number of security tools sold and protects over 415,000 customers worldwide.)

## Direct access to the internal network in under a minute

Another critical vulnerability that allows external attackers to penetrate the internal network in less than one minute was found by our security experts in Citrix products. Citrix applications are widely used in corporate networks, including for remote connection to workstations and critical business systems (for example, ERP) from any device online. This vulnerability allows any unauthorized user to not only access published applications, but also attack other resources of the company's internal network from the Citrix server. According to our estimate, **at least 80,000 companies from 158 countries are vulnerable**. If attackers had discovered this flaw before the security update was released, all these companies would have been at risk of compromise. We recommend companies to take security issues more seriously and regularly install security updates.

## ***Citrix vulnerability:*** one fifth of companies worldwide still at risk



**Vulnerable companies around the globe**
Number of vulnerable companies:

■ Less than 250
■ 250—999
■ 1,000—1,999
■ 2,000—4,999
■ 5,000—29,999
■ 30,000 or more

© Positive Technologies

## Opportunities for hackers to move through the corporate infrastructure

During the first four months of 2021, our experts discovered seven vulnerabilities in VMware products, half of which are of critical severity. For example, the most dangerous vulnerability in the vCenter Server virtual infrastructure management platform by VMware allows unauthorized users to execute arbitrary commands on the server. After successfully exploiting this vulnerability, attackers can develop the attack, move through the corporate network, and gain access to data stored in the compromised system (such as information about virtual machines and system users). If the vulnerable software can be accessed from the Internet (there are over 6,000 vulnerable VMware vCenter devices worldwide that are accessible online), this allows an external attacker to penetrate the company's infrastructure and gain access to sensitive data. It is worth noting that VMware products hold up to 80 percent of the virtual market and are used by more than four million users and 20,000 companies around the world.

## Remote server management

Server administration (such as installation of updates and software configuration) used to require the physical presence of a specialist to connect a monitor, keyboard, and mouse to the server and then perform the needed operations. Today, this task is handled by web interfaces accessible from any part of the world. One such remote administration tool is Cisco Integrated Management Controller. During the last three years, two critical vulnerabilities were found and fixed in this solution, one of them by Positive Technologies. This vulnerability allowed hackers to obtain access to the vulnerable system and perform arbitrary actions with maximum privileges, making it possible to obtain full control over the server infrastructure from the Internet at all companies that used such systems at the moment the security update was released.

## Access to encrypted data

For several years, Positive Technologies has been helping Intel to fix vulnerabilities. One such vulnerability was found in 2019 in the Intel CSME subsystem used for remote administration. The Intel CSME firmware implements EPID (Enhanced Privacy ID) remote attestation, allowing individual computers to be identified unambiguously and anonymously. By using this vulnerability, attackers can access encrypted data and not only decrypt it but spoof the victim's computer by fooling the authenticity checks. EPID is also used for protecting digital content, securing financial transactions, and performing IoT attestation. Most Intel chipsets released in the last five years contain this vulnerability. It is impossible to fix errors in firmware that is hard-coded in chipsets by simply updating this firmware: the chipset itself must be replaced.

## Technological process disruption

Recent years have seen a significant increase in the number of vulnerabilities discovered in industrial network equipment—switches, interface converters, and gateways. According to a report by Claroty, a company that specializes in industrial cybersecurity, 24.7 percent more vulnerabilities were discovered in ICS in 2020 than in the previous year.

Positive Technologies helped Siemens find and eliminate 23 vulnerabilities of high and critical severity in 2018–2021. These vulnerabilities included, for example, flaws in the CPU of Siemens SIMATIC S7-1500 programmable logic controllers (PLCs), used to automate process control in industries such as automotive production, food, chemicals, and other sectors. These vulnerabilities allowed an attacker to perform denial of service against a PLC and stop related industrial processes, causing production shutdown, damage to equipment, and/or industrial accidents. Such consequences can lead to tremendous losses.

## Full equipment control

In 2020, our experts discovered a vulnerability of the highest degree of danger in the BIG-IP application delivery controller, used by major companies across the world. By using this vulnerability, an attacker with access to the BIG-IP utility could execute commands and fully compromise the system. The attacker could create or delete files, disable services, intercept information, run arbitrary system commands and Java code, and further develop the attack against the internal network. This was particularly dangerous for companies whose F5 BIG-IP web interface is accessible from the Internet. At the time this research was published (June 2020), there were over 8,000 such devices worldwide.

## Withdrawing money from bank cards

Positive Technologies discovered dangerous vulnerabilities in Verifone point of sale (POS) terminals. Verifone is one of the largest providers of POS terminals in the world (7.6 billion transactions annually). Criminals could use these vulnerabilities to intercept payment card PINs, change the transaction amount on the terminal screen, send a request to the acquiring bank for withdrawing an arbitrary amount, and perform other malicious actions in 150 countries where such devices were used. Given the global scale of payment card theft and criminals' focus on the financial sector, attacks on vulnerable POS terminals threatened significant losses to banks and their clients.

This report has covered only a part of the most serious security problems our experts regularly discover in their daily work. The software and hardware products mentioned in this article are known to IT experts around the world, most of whom use them on a daily basis. These products are crucial for business. Imagine the consequences of attacks on companies where these products remain vulnerable. Attackers are constantly refining their tools, meaning that the fight against criminals is unwinnable without close cooperation between software vendors and information security experts. Without researchers and their initiatives, vendors would be left one-on-one against hackers. The process of detection and elimination of vulnerabilities would consist in quickly responding to cyberattacks and taking measures to eliminate their consequences. Companies that use vulnerable software would lose trust in manufacturers and seek safer alternatives.

Positive Technologies works diligently to make our digital environment a safer place. We are in constant daily communication with software and hardware vendors to help them improve their products, with researchers to share our knowledge and expertise (adhering to the principles of responsible disclosure), and with ordinary users to educate them about the perils of life in cyberspace. This is the contribution to the international infosec community that every cybersecurity company must make. And we are not planning to stop!

## About Positive Technologies

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

For 19 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.