Solutions Services Industries Company Our Thinking Case Studies Contact Us

Strategy →

Common types of security vulnerabilities & ways to fix them

By Nadejda Alkhaldi, Innovation Analyst

Published on July 6, 2022

A vulnerability in Microsoft’s Exchange Server contributed to a series of cyberattacks affecting over 60,000 private companies in the US. And just one

earlier, an aerospace company, Bombardier, had its employees and suppliers' data breached due to weaknesses in its third-party file app.

There are many security vulnerability types that can put your IT system on hackers' radar. From poor coding practices to defective external components, no matter what the reason is, many end up being exposed. To mitigate this issue, businesses benefit from QA and testing services to evaluate their own software and networks and assess the security risks of external vendor components.

which security vulnerability types may be exposing your system to cyberthreats at this very moment? How do vulnerabilities appear? And how can we mitigate them?

What is a software

and where does it originate from?

A security vulnerability is an unintended system or component characteristic that magnifies the risk of an intrusion or data loss, either by accidental exposure, intentional attack, or conflicts with new components.

be a design flaw, an implementation bug, a misconfiguration, etc.

Before we proceed any further, let’s clarify the difference between a vulnerability, an exploit, and a threat.

- **A vulnerability**

in the system without any efforts from outsiders

- **An exploit** is the way that intruders use an existing system weakness to mount an attack
- **A threat** is the actual incident when

multiple exploits use a vulnerability to penetrate a system

Security experts can eliminate vulnerabilities upon discovery using software patches, hardware replacement, and system reconfiguration. Training the end users on and keeping all components up to date will also prevent and minimize vulnerabilities. Additionally, the security teams need to keep in mind that as systems evolve, new weaknesses appear. Therefore, businesses need to scan software, hardware, and networks systematically for emerging vulnerabilities and fix them before they are discovered and exploited.

New security vulnerabilities keep emerging rapidly, as the US government's National Vulnerability Database (NVD)

8,000 new entries in the first quarter of 2022. With this rapid pace, many businesses can’t keep up and leave open weaknesses for years, exposing their systems. A study of software revealed that 75% of the attacks mounted in 2020 exploited exposures that were at least two years old, while 18% relied on weaknesses reported back in 2013!

How do security

get into software and networks?

According to research, 75% of applications developed by software vendors don’t comply with the Open Web Application Security Project (OWASP) Top 10 standards. These standards available. So, why are so many still failing to produce a safe application? Here are the main reasons:

1. **Vulnerable third-party code and other components.** It's a common practice to reuse third-

as this speeds up the development process significantly. However, users tend to take the security of these parts lightly, and often deploy them without thorough evaluation. The same to copy-pasting code from sources, such as Stack Overflow, without assessing its safety.

2. **Insecure coding practices.** Recent studies show that security is not even on the radar for

In an experiment exploring the attitude of 1,200 developers, researchers concluded that only 14% view security as a priority when writing code. Also, note that many organizations demand their developers code fast under tight deadlines, which simply doesn’t leave room for thorough security evaluation and results in code vulnerabilities.

3. **Rapidly changing cyberattack landscape.** Attackers are constantly discovering

ways to breach applications' security. So, parts that were considered immune before can become vulnerable today. If the IT team doesn't systematically assess applications and networks for vulnerabilities, and doesn't software up to date, it’s just a matter of time until weaknesses start emerging.

Security vulnerability types classification

There are two platforms, OWASP and CWE, that offer a and detailed security vulnerabilities list. They update their listings to include any emerging weaknesses. Both resources can be used to educate programmers, testers, and engineers.

OWASP is a non-profit global

regularly publishes OWASP top 10 software vulnerabilities list. Common Weakness Enumeration (CWE) is a composition of software and hardware vulnerabilities also developed by a dedicated community, and it includes 25 entries.

of the most prominent security vulnerabilities that we want to highlight in this article, sorted by domain. These can manifest themselves in any IT system, such as the cloud, IoT-based configurations, and mobile apps.

Network-based	OS-based	Hu
Unencrypted data	Misconfigured system components	Ru vir
Sensitive data exposure	Weak server-side control	We
Insufficient transport layer protection	Remote code execution	Us vu
	Known OS-based vulnerabilities	Ins

1. Lack of strong encryption practices

Even though encryption would not stop

cyberattack, it is essential to ensure that sensitive data remains safe even if its storage platform is breached. Attackers can’t misuse encrypted data until they decode it, which gives the violated business necessary measures, such as notify the impacted parties and prepare identity theft countermeasures.

Research shows that many companies have no immediate plans of encrypting data on USB sticks, laptops, and desktops.

of data protection regulations, GDPR doesn’t explicitly require encryption, but describes it as “appropriate technical and organizational measures” for data safety.

In its Cost of a Data Breach report, IBM pointed out that encryption most impactful factors that can reduce the average cost of data breaches.