# 9 Types OF SECURITY VULNERABILITIES

Balbix®

## SECURITY VULNERABILITY:

A WEAKNESS WHICH CAN BE EXPLOITED BY A THREAT ACTOR, SUCH AS AN ATTACKER, TO PERFORM UNAUTHORIZED ACTIONS WITHIN A COMPUTER SYSTEM.

TO EXPLOIT A VULNERABILITY, AN ATTACKER MUST HAVE AT LEAST ONE APPLICABLE TOOL OR TECHNIQUE THAT CAN CONNECT TO A SYSTEM WEAKNESS.

Vulnerability is a very broad term. Yet somehow, in infosec, we've come to narrowly associate a vulnerability with unpatched software and misconfigurations.

## HERE ARE 9 TYPES OF SECURITY VULNERABILITIES

### UNPATCHED SOFTWARE

Unpatched vulnerabilities allow attackers to run a malicious code by leveraging a known security bug that has not been patched. The adversary will try to probe your environment looking for unpatched systems, and then attack them directly or indirectly.

### MISCONFIGURATION

System misconfigurations (e.g. assets running unnecessary services, or with vulnerable settings such as unchanged defaults) can be exploited by attackers to breach your network. The adversary will try to probe your environment looking for systems that can be compromised due to some misconfiguration, and then attack them directly or indirectly.

### WEAK CREDENTIALS

An attacker may use dictionary or brute force attacks to attempt to guess weak passwords, which can then be used to gain access to systems in your network.

### PHISHING, WEB & RANSOMWARE

Phishing is used by attackers to get users to inadvertently execute some malicious code, and thereby compromise a system, account or session. The adversary will send your users a link or malicious attachment over email (or other messaging system), often alongside some text/image that entices them to click.

### MALICIOUS INSIDER

An employee or a vendor who might have access to your critical systems can decide to exploit their access to steal or destroy information or impair them. This is particularly important for privileged users and critical systems.

### COMPROMISED CREDENTIALS

An attacker can use compromised credentials to gain unauthorized access to a system in your network. The adversary will try to some-how intercept and extract passwords from unencrypted or incorrectly encrypted communication between your systems, or from unsecured handling by software or users. The adversary may also exploit reuse of passwords across different systems.

### TRUST RELATIONSHIP

Attackers can exploit trust configurations that have been set up to permit or simplify access between systems (e.g. mounted drives, remote services) to propagate across your network. The adversary, after gaining access to a system, can then proceed to breach other systems that implicitly trust the originally compromised system.

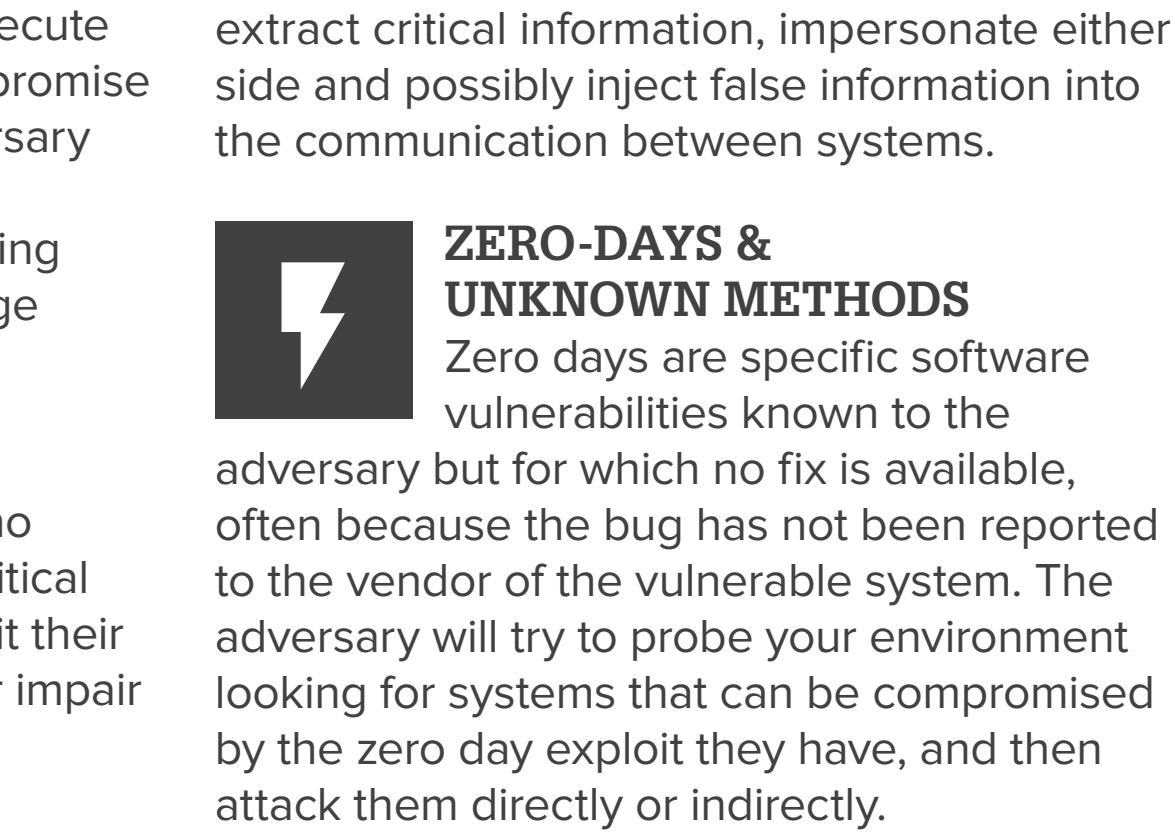
### MISSING/POOR ENCRYPTION

With attacks on Missing/Poor Encryption, an attacker can intercept communication between systems in your network and steal information. The attacker can intercept unencrypted or poorly encrypted information and can then extract critical information, impersonate either side and possibly inject false information into the communication between systems.

### ZERO-DAYS & UNKNOWN METHODS

Zero days are specific software vulnerabilities known to the adversary but for which no fix is available, often because the bug has not been reported to the vendor of the vulnerable system. The adversary will try to probe your environment looking for systems that can be compromised by the zero day exploit they have, and then attack them directly or indirectly.

Balbix looks at all 9 classes of vulnerabilities, automatically and continuously calculating likelihood of breach via each class for every asset on your network. The result is mapped to the Balbix Breach Method matrix, and used as part of the risk calculation score that feeds actionable, prioritized insights to help your team maximize cyber resilience.




**LEARN MORE** about how Balbix can help.

Balbix® AI-POWERED CYBERSECURITY POSTURE TRANSFORMATION