9 Types

OF

SECURITY VULNERABILITIES

Balbix®

9 Types OF SECURITY VULNERABILITIES

The dictionary defines a vulnerability as “the quality or state of being exposed to the possibility of being attacked or harmed.” Wikipedia defines a security vulnerability as “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.

The reason is that 20+ years ago (think pre-Google), when traditional vulnerability management vendors were getting their start, they focused on unpatched software and misconfiguration, the press and analysts branded this functionality, “vulnerability management,” and here we are 2 decades later living with that definition. We even have a de facto standard severity ranking system, CVSS scores, that handle only this narrow definition.

The problem is that not every vulnerability is a CVE with a corresponding CVSS score.

If you consider the broader, dictionary definition of a vulnerability, it is anything that exposes you and puts you at risk. The enterprise attack surface is exploding with assets including thousands of devices, apps and users, susceptible to hundreds of attack vectors, ranging from simple things like weak passwords, to more complex things like phishing, unpatched software, encryption and configuration issues, etc.

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.

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.

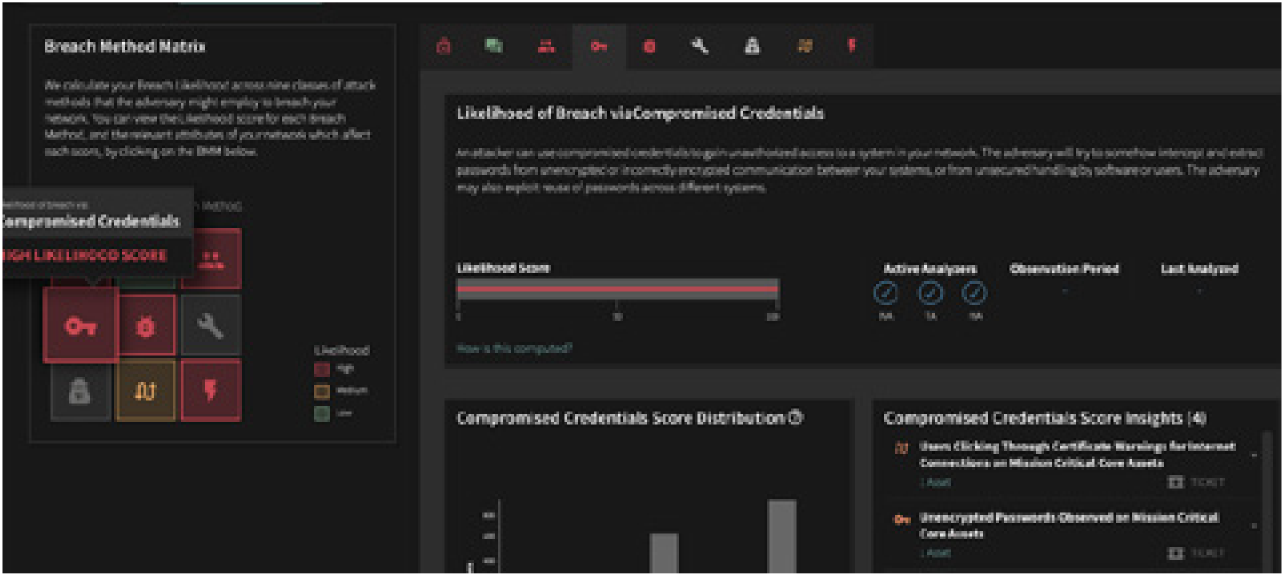
COMPROMISED CREDENTIALS An attacker can use compromised credentials to gain unauthorized access to a system in your network. The adversary will try to somehow intercept and extract passwords from unencrypted or incorrectly encrypted communication between your systems, or from unsecured handling by software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

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.

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.



Breach Method Matrix

We calculate your Breach Likelihood across nine classes of attack methods that the adversary might employ to breach your network. You can view the Likelihood score for each Breach Method, and the relevant attributes of your network which affect each score, by clicking on the BMM below.

Method of breach via Compromised Credentials

HIGH LIKELIHOOD SCORE

Likelihood: High, Medium, Low

Likelihood of Breach viaCompromised Credentials

An attacker can use compromised credentials to gain unauthorized access to a system in your network. The adversary will try to somehow 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.

Likelihood Score

Active Analyzers	Observation Period	Last Analyzed
NA NA NA	-	-

How is this computed?

Compromised Credentials Score Distribution

Compromised Credentials Score Insights (4)

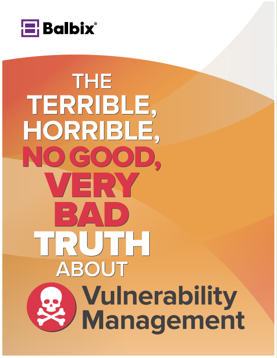
- Users Clicking Through Certificate Warnings for Internet Connections on Mission Critical Core Assets — 1 Asset — TICKET
- Unencrypted Passwords Observed on Mission Critical Core Assets — 1 Asset — TICKET

LEARN MORE

about how Balbix can help.

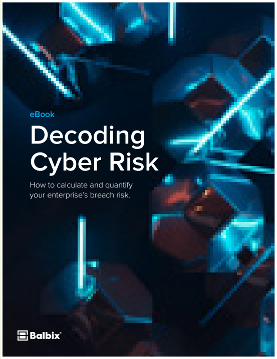
LEARN MORE

about Vulnerability Management.



Balbix

THE TERRIBLE, HORRIBLE, NO GOOD, VERY BAD TRUTH ABOUT Vulnerability Management



eBook

Decoding Cyber Risk

How to calculate and quantify your enterprise's breach risk.

Balbix