edgescan™

January 2022 Vulnerability Snapshot

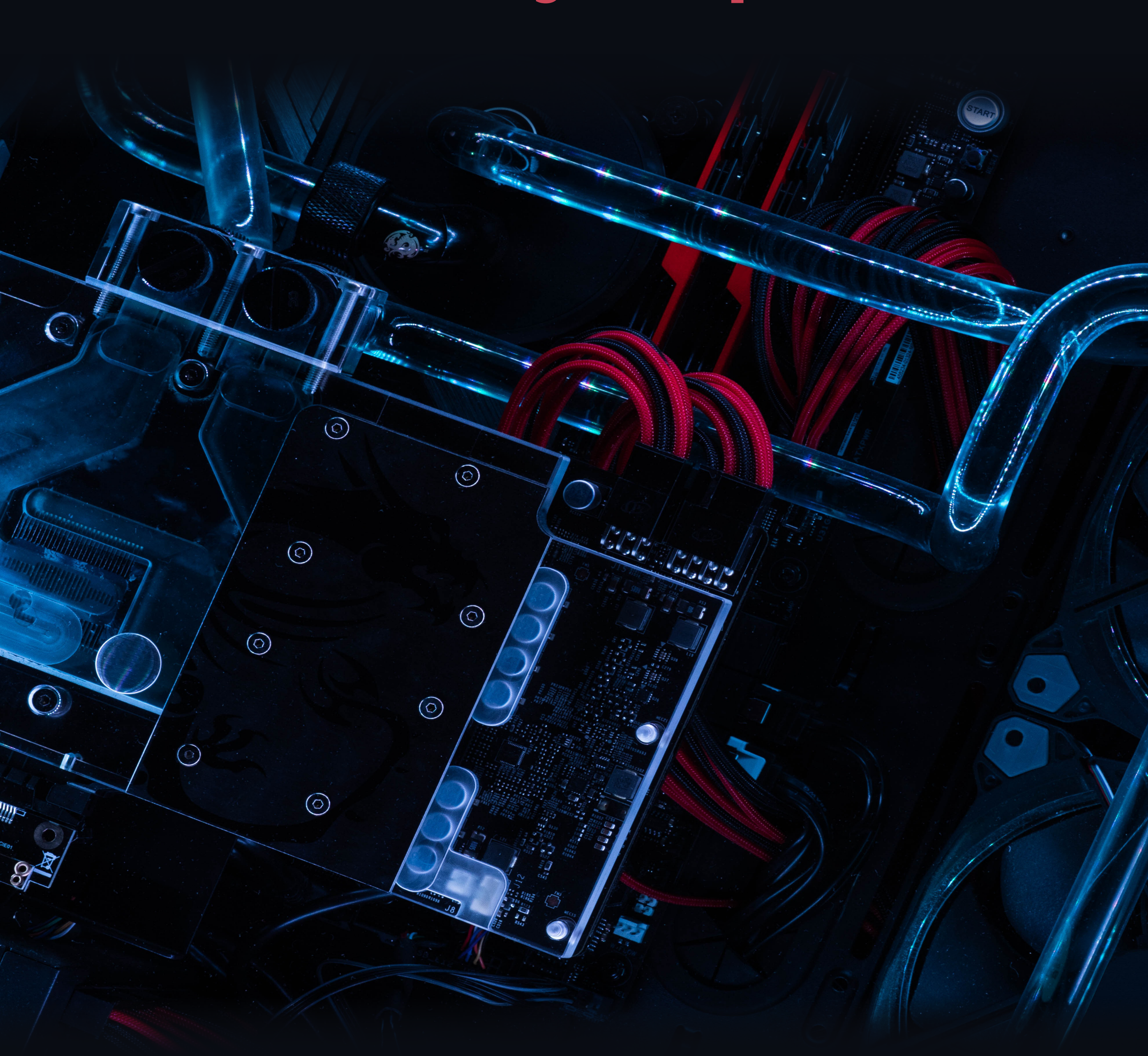


Table of Contents

Table of contents

Introduction

This year we are introducing a new way to keep the infosec community up to date on the latest vulnerabilities and the various CVEs associated with these vulnerabilities. We break down by Network/Device and Application/API and the percentages of each vulnerability that we have discovered during this month through the Edgescan platform.

Percentages

Full Stack

Critical	7.0%
High	12.6%
Medium	57.1%

Network/Device

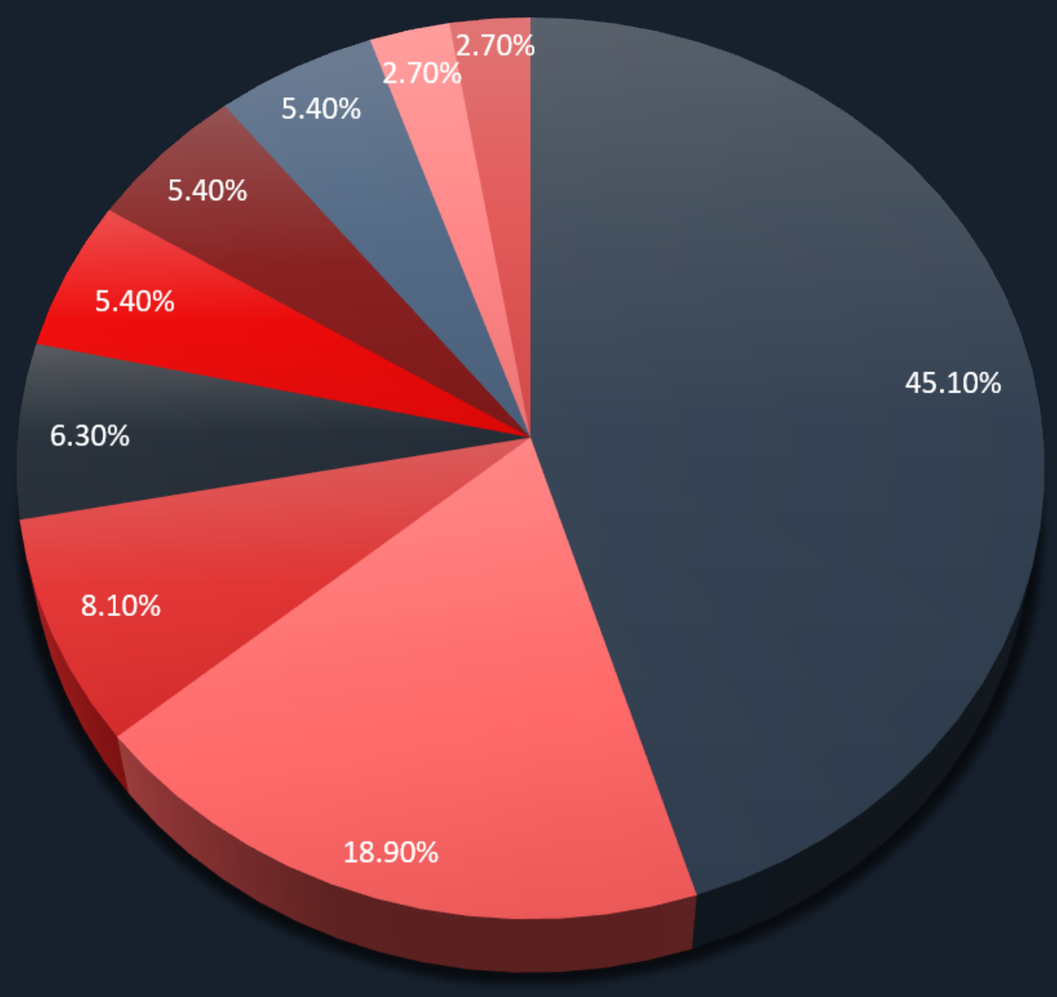
Critical	8.8%
High	16.9%
Medium	74.3%

Application/API

Critical	16.0%
High	7.4%
Medium	76.5%

Application/API
Most Common High & Critical Risks

Vulnerabilities	%
SQL injection	45.1%
Cross-site scripting (stored)	18.9%
Brute Forcing Possible	8.1%
BOLA/IDOR - Insecure Direct Object Reference	6.3%
Cross-Site Scripting - XSS (reflected)	5.4%
Email spoofing	5.4%
Sensitive File(s) Disclosure	5.4%
Malicious File Upload	2.7%
Debugging enabled	2.7%



SQL injection

Vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

Various attacks can be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and executing operating system commands.

Cross-site scripting (stored)

Insufficient encoding of user input exposes the application to persistent cross site scripting (XSS) vulnerabilities.

These vulnerabilities enable potentially dangerous input from the user to be accepted by the application and then embedded back in the HTML response of the page returned by the web server.

This code is then read by the client web browser and executed as script.

The type of cross site scripting found in this application is known as ‘persistent’ or ‘stored’ cross site scripting and is commonly used in conjunction with attacks on end users such as Phishing.

Brute Forcing Possible

It was possible to perform a brute forcing attack on the users of this web application. A common attack by malicious users is to attempt a number of different combinations of passwords, IDs or 2FA codes in order to gain unauthorized access to an account or user data.

BOLA/Insecure Direct Object Reference (IDOR)

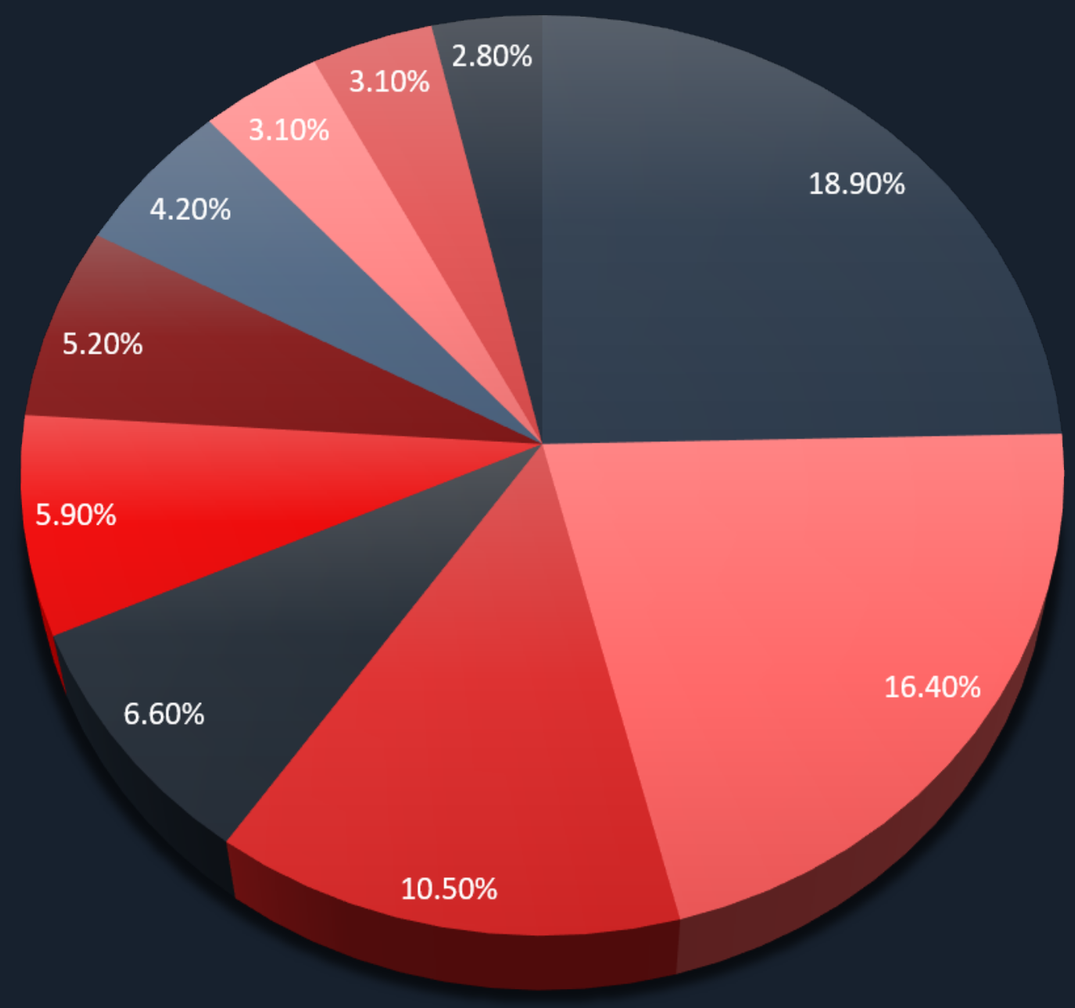
When an application exposes a reference to an internal asset.

The most common example of IDOR (although is not limited to this one) is a record identifier in a storage system such as a database, filesystem or other data source.

Network/Device

Most Common High & Critical Risks

Vulnerabilities	%
PHP Multiple Vulnerabilities	18.9%
Oracle Java Multiple Vulnerabilities(Windows)	16.4%
OS End Of Life Detection	10.5%
Log4Shell Multiple CVEs	6.6%
Apache HTTP Server Multiple Vulnerabilities - Windows	5.9%
VMware vCenter Server 6.5, 6.7, 7.0 Multiple Vulnerabilities	5.2%
Apache Tomcat Multiple Vulnerabilities	4.2%
Cisco Smart Install Protocol Misuse	3.1%
Microsoft Windows Multiple Vulnerabilities (KB5005565)	3.1%
MariaDB End Of Life Detection (Windows)	2.8%



PHP Multiple Vulnerabilities:

Known vulnerabilities such as:

CVE-2011-3379, CVE-2011-4566, CVE-2011-4885, CVE-2012-0057, CVE-2012-0781, CVE-2012-0788, CVE-2012-0789, CVE-2019-11044, CVE-2019-11045, CVE-2019-11046, CVE-2019-11047, CVE-2019-11050, CVE-2020-7059, CVE-2020-7060, CVE-2021-21702, CVE-2018-1000860, CVE-2018-1000869, CVE-2018-1000870, CVE-2019-1000010, CVE-2020-5504

Oracle Java Multiple Vulnerabilities(Windows)

Known vulnerabilities such as:

CVE-2010-4467, CVE-2012-1711, CVE-2012-1713, CVE-2012-1718, CVE-2012-1719, CVE-2012-1720, CVE-2012-1723, CVE-2015-0458, CVE-2018-2790, CVE-2018-2794, CVE-2018-2795, CVE-2018-2797, CVE-2018-2798, CVE-2018-2814, CVE-2018-2815

OS End Of Life Detection:

Detection of unsupported operating systems which pose a risk due to multiple vulnerabilities and lack of maintenance.

Log4Shell Multiple CVEs

Apache Log4j2 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

CVE-2021-44228, CVE-2021-45046, CVE-2021-44228, CVE-2021-44228, CVE-2021-44228, CVE-2021-45046

Apache HTTP Server Multiple Vulnerabilities – Windows

Known vulnerabilities such as::

CVE-2021-31618 CVE-2021-34798, CVE-2021-39275, CVE-2021-40438, CVE-2021-34798, CVE-2021-39275, CVE-2021-40438, CVE-2021-44790, CVE-2021-44224, CVE-2016-5387, CVE-2017-9788

VMware vCenter Server 6.5, 6.7, 7.0 Multiple Vulnerabilities

Known vulnerabilities such as:

CVE-2021-44228, CVE-2021-45046 CVE-2021-21980, CVE-2021-22049, CVE-2021-22048