Vulnerability Scanning - DIGITAL EDUCATION PLATFORM SERVER April 24

Generated on April 27, 2023 at 11:05 AM EAT

Biubwa Ameir [ameib001]
VODACOM TANZANIA

Confidential: The following report contains confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.

Table of Contents

About This Report

Unaddressed vulnerabilities on hosts can provide attackers with easier access to an otherwise secure network. Determining and implementing remediation measures is key to properly securing any network.

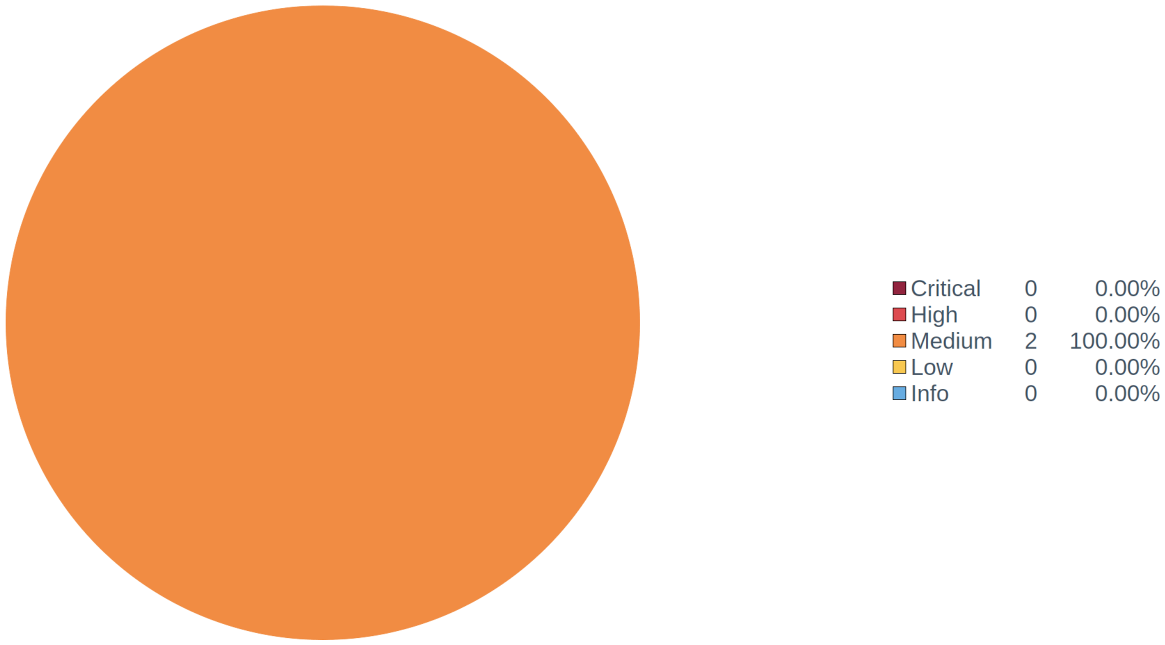
The Remediation Instructions by Host report provides detailed information on the most vulnerable hosts identified on the network. The report is organized into Active and Passive and broken down by host. For each of the vulnerable hosts, detailed steps to mitigate the risk of the vulnerabilities, including CVE, BID, and vendor knowledgebase articles, are provided. Additionally, this report provides information about the top services and ports on each vulnerable host.

Executive Summary

This chapter provides an overview of the vulnerability statuses of hosts covered in this report.

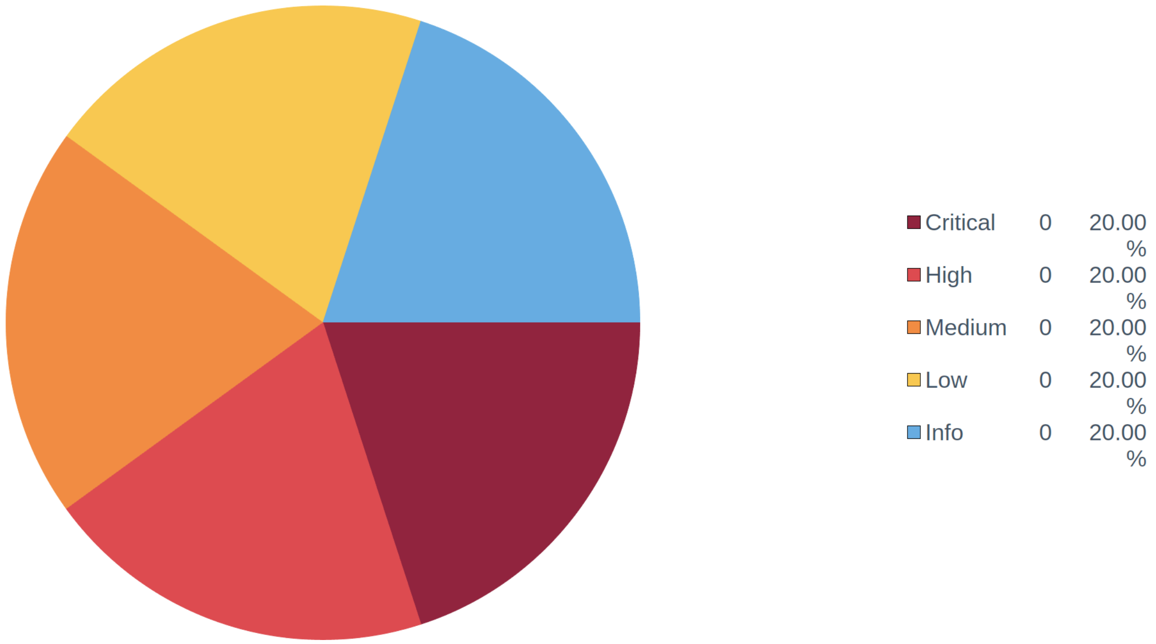
The Active Vulnerability Summary pie chart depicts the breakdown of vulnerability severities detected by active scanning. The Active Vulnerability Summary table presents an overview of the active vulnerabilities detected within an organization’s network by subnet. T

Active Vulnerability Summary



The Passive Vulnerability Summary pie chart depicts the breakdown of vulnerability severity detected by passive scanning. The Passive Vulnerability Summary table presents an overview of the active vulnerabilities detected.

Passive Vulnerability Summary



Active Remediation Instructions by Host

This chapter provides vulnerable hosts discovered through active scanning. Active vulnerability scanning uses Nessus to send packets to target machines, providing a snapshot of the network services and applications installed. Active scanning also determines whether vulnerabilities are present. Active scanning can perform highly accurate patch, configuration, and vulnerability audits across many systems, including Unix, Linux, Windows, network devices, and database systems.

Summary

IP Address	DNS Name	OS CPE	Score	Total	Vulns
10.8.45.10	vtzmbzdepuat01.vodacomtz.corp	cpe:/o:redhat:enterprise_linux:7:update9:es	6	2	2

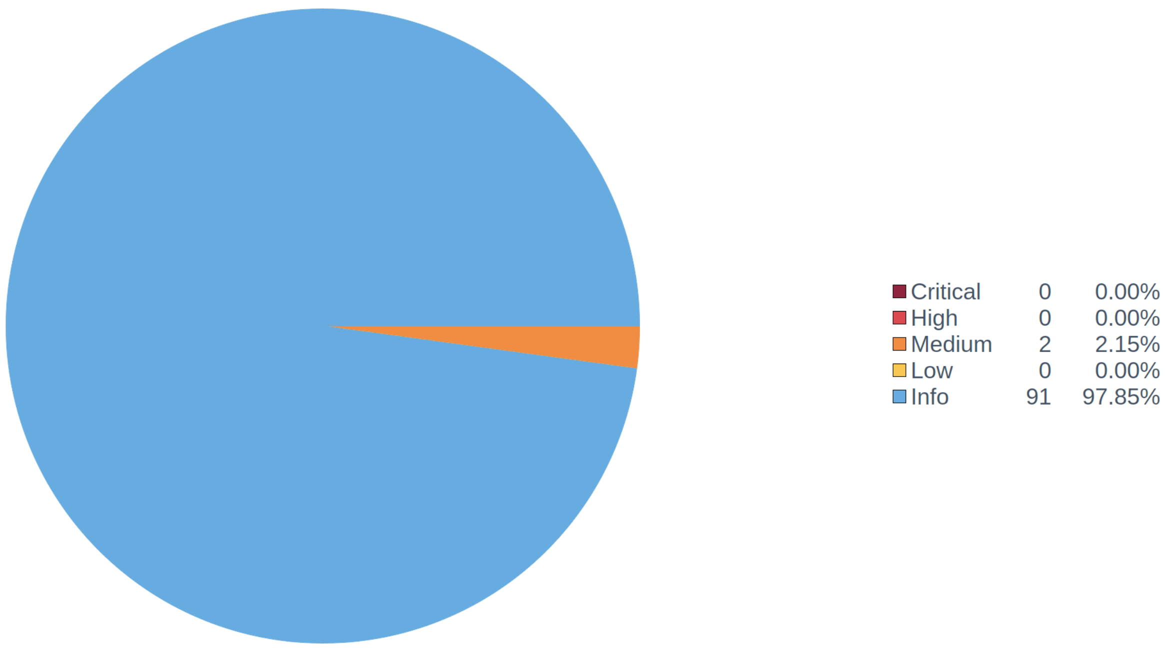
This section uses an iterator to provide detailed information about each of the top 20 most vulnerable hosts by score. The vulnerability score for each host is calculated by totaling the count of vulnerabilities at each severity level then multiplying it by the severity score. The default severity scores are: Info - 0, Low – 1, Medium – 3, High – 10, Critical – 40.

The Vulnerability Summary pie chart shows the ratio of vulnerabilities by severity detected on that host.

10.8.45.10

IP Address: 10.8.45.10
DNS Name: vtzmbzdepuat01.vodacomtz.corp
Score: 6
High: 0
Crit.: 0
Total: 93

Vulnerability Summary



Top Services Discovered

Service	Count
A web server is running on this port.	2
An SSH server is running on this port.	1
Process ID : 10617 / Executable : /usr/libexec/docker/docker-proxy-current / Command line : /usr/libexec/docker/docker-proxy-current -proto tcp -host-ip 0.0.0.0 -host-port 5432 -container-ip 172.22.0.2 -container-port 5432	1

Service	Count
Process ID : 11695 / Executable : /usr/libexec/docker/docker-proxy-current / Command line : /usr/libexec/docker/docker-proxy-current -proto tcp -host-ip 0.0.0.0 -host-port 8483 -container-ip 172.17.0.2 -container-port 80	1
Process ID : 1487 / Executable : /usr/sbin/sshd / Command line : /usr/sbin/sshd -D	1
Process ID : 1490 / Executable : /usr/sbin/httpd / Command line : /usr/sbin/httpd -DFOREGROUND	1
Process ID : 2318 / Executable : /opt/Symantec/sdcssagent/IPS/bin/sisipsdaemon / Command line : /opt/Symantec/sdcssagent/IPS/bin/sisipsdaemon	1
Process ID : 8572 / Executable : /usr/sbin/rsyslogd / Command line : /usr/sbin/rsyslogd -n	1

Top Port Findings

Port	Score	Info	Low	Med.	High	Crit.	Total
80	6	13	0	2	0	0	15
36179	0	2	0	0	0	0	2
8483	0	11	0	0	0	0	11
5432	0	3	0	0	0	0	3
2222	0	2	0	0	0	0	2
22	0	12	0	0	0	0	12
0	0	48	0	0	0	0	48

Vulnerability Listing

Plugin Name	Severity	Total
HTTP TRACE / TRACK Methods Allowed	Medium	1
Git Repository Served by Web Server	Medium	1

Remediation Plan

Plugin Name	Severity	Port	Exploit?
Git Repository Served by Web Server	Medium	80	No
Synopsis: The remote web server may disclose information due to a configuration weakness.			
Description: The web server on the remote host allows read access to a Git repository. This potential flaw can be used to download content from the Web server that might otherwise be private.			
Solution: Verify that the listed Git repositories are served intentionally.			
See Also: https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d http://www.nessus.org/u?b573eafc			
CVE:			
BID:			
Cross References:			
First Discovered: Mar 30, 2023 11:36:53 EAT			
Last Observed: Apr 24, 2023 18:51:05 EAT			
Exploit Frameworks:			

Plugin Name	Severity	Port	Exploit?
HTTP TRACE / TRACK Methods Allowed	Medium	80	No

Synopsis: Debugging functions are enabled on the remote web server.

Description: The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution: Disable these HTTP methods. Refer to the plugin output for more information.

See Also: https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
https://download.oracle.com/sunalerts/1000718.1.html

CVE: CVE-2003-1567,CVE-2004-2320,CVE-2010-0386

BID: 9506,9561,11604,33374,37995

Cross References: CERT #288308,CERT #867593,CWE #16,CWE #200

First Discovered: Mar 30, 2023 11:36:53 EAT

Last Observed: Apr 24, 2023 18:51:05 EAT

Exploit Frameworks:

Passive Remediation Instructions by Host

This chapter provides a summary of the vulnerable hosts discovered through passive scanning. The Passive Vulnerability Scanner (PVS) is an advanced network monitoring application designed to detect vulnerabilities on the network by listening to network communications. Through passive monitoring, PVS can reveal devices and software on the network that are not authorized, or that may indicate a network compromise.

Summary

IP Address	DNS Name	OS CPE	Score	Total	Vulns

This section uses an iterator to provide detailed information about each of the top 20 most vulnerable hosts by score. The vulnerability score for each host is calculated by totaling the count of vulnerabilities at each severity level then multiplying it by the severity score. The default severity scores are: Info - 0, Low – 1, Medium – 3, High – 10, Critical – 40. Administrators can customize the severity scores as necessary. For each host, several components are included.

The Vulnerability Summary pie chart shows the ratio of vulnerabilities by severity detected on that host.