X3rror

IOT & Security Sol's

Security Assessment Finding Report

Business Confidential

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for host, the report describes every issue found. Please consider the advice given in description, in order to rectify the issue. Vendor security updates are not trusted. Overrides are off. Even when a result has an override, this report uses the actual threat of the result. Information on overrides is included in the report. Notes are included in the report. This report might not show details of all issues that were found. Issues with the threat level "High" are not shown. Issues with the threat level "Medium" are not shown. Issues with the threat level "Low" are not shown. Issues with the threat level "Log" are not shown. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown. This report contains all 7 results selected by the filtering described above. Before filtering there were 8 results. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Testing Results For 172.162.217.137 Phase by phase

Date : Aug. 11, 2020, 8:30 p.m.

1.Scanning

Phase 1

Port	Protocol	Service	Service Version	Product
21	tcp	ftp	2.3.4	vsftpd
22	tcp	ssh	4.7p1 Debian 8ubuntu1	OpenSSH
23	tcp	telnet	na	Linux telnetd
25	tcp	smtp	na	Postfix smtpd
53	tcp	domain	9.4.2	ISC BIND
80	tcp	http	2.2.8	Apache httpd
111	tcp	rpcbind	2	na
139	tcp	netbios-ssn	3.X - 4.X	Samba smbd
445	tcp	netbios-ssn	3.X - 4.X	Samba smbd
512	tcp	exec	na	netkit-rsh rexecd
513	tcp	login	na	na
514	tcp	shell	na	Netkit rshd
1099	tcp	java-rmi	na	GNU Classpath grmiregistry
1524	tcp	bindshell	na	Metasploitable root shell
2049	tcp	nfs	2-4	na
2121	tcp	ftp	1.3.1	ProFTPD
3306	tcp	mysql	5.0.51a-3ubuntu5	MySQL
5432	tcp	postgresql	8.3.0 - 8.3.7	PostgreSQL DB
5900	tcp	vnc	na	VNC
6000	tcp	X11	na	na
6667	tcp	irc	na	UnrealIRCd
8009	tcp	ajp13	na	Apache Jserv
8180	tcp	http	1.1	Apache Tomcat/Coyote JSP engine

2.Vulnerability Scan

Phase 2

Port	Protocol	CVSS	CVE	Severity	Vul Name	Impact	Summary
2121	tcp	4.8	NOCVE	Medium	FTP Unencrypted Cleartext Login	An attacker can uncover login names and passwords by sniffing traffic to the FTP service.	The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
25	tcp	4.3	CVE-2014-3566	Medium	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.	This host is prone to an information disclosure vulnerability.
514	tcp	7.5	NOCVE	High	rsh Unencrypted Cleartext Login		This remote host is running a rsh service.
21	tcp	7.5	NOCVE	High	vsftpd Compromised Source Packages Backdoor Vulnerability	Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.	vsftpd is prone to a backdoor vulnerability.
22	tcp	2.6	NOCVE	Low	SSH Weak MAC Algorithms Supported		The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.
23	tcp	4.8	NOCVE	Medium	Telnet Unencrypted Cleartext Login	An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.	The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.
3632	tcp	9.3	CVE-2004-2687	High	DistCC Remote Code Execution Vulnerability	DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.	DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.
6667	tcp	6.8	CVE-2016-7144	Medium	UnrealIRCd Authentication Spoofing Vulnerability	Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.	This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability.
445	tcp	6.0	CVE-2007-2447	Medium	Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.	Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-

							supplied input.
1099	tcp	10.0	NOCVE	High	Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.	Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.
1524	tcp	10.0	NOCVE	High	Possible Backdoor: Ingreslock	Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.	A backdoor is installed on the remote host.
5900	tcp	4.8	NOCVE	Medium	VNC Server Unencrypted Data Transmission	An attacker can uncover sensitive data by sniffing traffic to the VNC server.	The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.
5432	tcp	4.3	CVE-2014-3566	Medium	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.	This host is prone to an information disclosure vulnerability.
6200	tcp	7.5	NOCVE	High	vsftpd Compromised Source Packages Backdoor Vulnerability	Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.	vsftpd is prone to a backdoor vulnerability.
8009	tcp	7.5	CVE-2020-1938	High	Apache Tomcat AJP RCE Vulnerability (Ghostcat)		Apache Tomcat is prone to a remote code execution vulnerability in the AJP connector dubbed 'Ghostcat'.
3306	tcp	9.0	NOCVE	High	MySQL / MariaDB weak password		It was possible to login into the remote MySQL as root using weak credentials.
80	tcp	10.0	CVE-2008-5304, CVE-2008-5305	High	TWiki XSS and Command Execution Vulnerabilities	Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.	The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.
512	tcp	10.0	NOCVE	High	rexec Passwordless / Unencrypted Cleartext Login		This remote host is running a rexec service.
8787	tcp	10.0	NOCVE	High	Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.	Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.
513	tcp	7.5	NOCVE	High	rlogin Passwordless / Unencrypted Cleartext		This remote host is running a rlogin service.

					Login		

3.Exploitation

Phase 3

Scan ID	CVE	Port	Protocol	Severity	Exploit
189	CVE-2007-2447	445	tcp	Medium	exploit/multi/samba/usermap_script
189	CVE-2004-2687	3632	tcp	High	exploit/unix/misc/distcc_exec

This report was automatically generated.