Rapport de Sécurité

Généré le: 27/06/2024 20:22:49

Introduction:

Ce rapport vise à présenter les vulnérabilités identifiées suite à un scan de sécurité. Les informations suivantes détaillent les services détectés, les versions associées, ainsi que les vulnérabilités (CVE) trouvées. Des recommandations sont également fournies pour remédier à ces vulnérabilités.

Host: 192.168.19.134

Port	Service	Version	CVE
21	ftp	vsftpd 2.3.4	CVE-2011-2523
22	ssh	OpenSSH 4.7p1 Debian 8ubuntu1	
23	telnet	Linux telnetd	CVE-2000-1195, CVE-2020-8797, CVE-2021-27171, CVE-2022-39028
25	smtp	Postfix smtpd	CVE-2004-0925, CVE-2005-0337, CVE-2023-51764, CVE-2024-27305
53	domain	ISC BIND 9.4.2	CVE-2008-0122, CVE-2008-4163
80	http	Apache httpd 2.2.8	
111	rpcbind	2	CVE-2003-1070
139	netbios-ssn	Samba smbd 3.X - 4.X	
445	netbios-ssn	Samba smbd 3.X - 4.X	
512	exec	netkit-rsh rexecd	
513	login	OpenBSD or Solaris rlogind	
514	tcpwrapped		CVE-1999-0095, CVE-1999-0082, CVE-1999-1471, CVE-1999-1122, CVE-1999-1467, CVE-1999-1506, CVE-1999-0084, CVE-2000-0388, CVE-1999-0209, CVE-1999-1198
1099	java-rmi	GNU Classpath grmiregistry	
1524	bindshell	Metasploitable root shell	
2049	nfs	2-4	CVE-2019-15491
2121	ftp	ProFTPD 1.3.1	CVE-2008-4242
3306	mysql	MySQL 5.0.51a-3ubuntu5	
5432	postgresql	PostgreSQL DB 8.3.0 - 8.3.7	

5900	vnc	VNC	CVE-2001-1422, CVE-2002-0971, CVE-2002-0994, CVE-2002-1336, CVE-2002-2088, CVE-2002-1511, CVE-2006-1652, CVE-2006-4309, CVE-2007-0756, CVE-2007-0998
6000	X11		CVE-2000-1169, CVE-2002-0402, CVE-2002-0517, CVE-2004-0157, CVE-2004-2097, CVE-2005-0084, CVE-2005-3248, CVE-2006-0577, CVE-2006-0745, CVE-2006-3470
6667	irc	UnrealIRCd	CVE-2004-0679, CVE-2006-1214, CVE-2009-4893, CVE-2010-2075, CVE-2013-6413, CVE-2013-7384, CVE-2016-7144, CVE-2017-13649, CVE-2023-50784
8009	ajp13	Apache Jserv	CVE-2000-1247, CVE-2020-1938
8180	http	Apache Tomcat/Coyote JSP engine 1.1	

Description des CVE:

CVE ID	Description	Recommandations
CVE-2011-2523	vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.	http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html
CVE-2000-1195	telnet daemon (telnetd) from the Linux netkit package before netkit-telnet-0.16 allows remote attackers to bypass authentication when telnetd is running with the -L command line option.	http://www.caldera.com/support/security/advisories/CSSA-2000-008.0.txt
CVE-2020-8797	Juplink RX4-1500 v1.0.3 allows remote attackers to gain root access to the Linux subsystem via an unsanitized exec call (aka Command Line Injection), if the undocumented telnetd service is enabled and the attacker can authenticate as admin from the local network.	https://cerne.xyz/bugs/CVE-2020-8797.html
CVE-2021-27171	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to start a Linux telnetd as root on port 26/tcp by using the CLI interface commands of ddd and shell (or tshell).	https://pierrekim.github.io/blog/2021-01-12-fiberhome-ont-0day-vulnerabilities.html#telnet-cli-privilege-escalation
CVE-2022-39028	telnetd in GNU Inetutils through 2.3, MIT krb5-appl through 1.0.3, and derivative works has a NULL pointer dereference via 0xff 0xf7 or 0xff 0xf8. In a typical installation, the telnetd application would crash but the telnet service would remain available through inetd. However, if the telnetd appli...	https://git.hadrons.org/cgit/debian/pkgs/inetutils.git/commit/?id=113da8021710d871c7dd72d2a4d5615d42d64289
CVE-2004-0925	Postfix on Mac OS X 10.3.x through 10.3.5, with SMTPD AUTH enabled, does not properly clear the username between authentication attempts, which allows users with the longest username to prevent other valid users from being able to authenticate.	http://lists.apple.com/archives/security-announce/2004/Oct/msg00000.html
CVE-2005-0337	Postfix 2.1.3, when /proc/net/if_inet6 is not available and permit_mx_backup is enabled in smtpd_recipient_restrictions, allows remote attackers to bypass e-mail restrictions and perform mail relaying by sending mail to an IPv6 hostname.	http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=267837

CVE ID	Description	Recommandations
CVE-2023-51764	Postfix through 3.8.5 allows SMTP smuggling unless configured with smtpd_data_restrictions=reject_unauth_pipelining and smtpd_discard_ehlo_keywords=chunking (or certain other options that exist in recent versions). Remote attackers can use a published exploitation technique to inject e-mail messages...	http://www.openwall.com/lists/oss-security/2023/12/24/1
CVE-2024-27305	aiosmtpd is a reimplementation of the Python stdlib smtpd.py based on asyncio. aiosmtpd is vulnerable to inbound SMTP smuggling. SMTP smuggling is a novel vulnerability based on not so novel interpretation differences of the SMTP protocol. By exploiting SMTP smuggling, an attacker may send smuggle/s...	https://github.com/aio-libs/aiosmtpd/commit/24b6c79c8921cf1800e27ca144f4f37023982bbb
CVE-2008-0122	Off-by-one error in the inet_network function in libbind in ISC BIND 9.4.2 and earlier, as used in libc in FreeBSD 6.2 through 7.0-PRERELEASE, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted input that triggers memory corruption...	http://lists.opensuse.org/opensuse-security-announce/2008-03/msg00004.html
CVE-2008-4163	Unspecified vulnerability in ISC BIND 9.3.5-P2-W1, 9.4.2-P2-W1, and 9.5.0-P2-W1 on Windows allows remote attackers to cause a denial of service (UDP client handler termination) via unknown vectors.	http://marc.info/?l=bind-announce&m;=122180244228376&w;=2
CVE-2003-1070	Unknown vulnerability in rpcbind for Solaris 2.6 through 9 allows remote attackers to cause a denial of service (rpcbind crash).	http://secunia.com/advisories/8685/
CVE-1999-0095	The debug command in Sendmail is enabled, allowing attackers to execute commands as root.	http://seclists.org/fulldisclosure/2019/Jun/16
CVE-1999-0082	CWD ~root command in ftpd allows root access.	http://www.alw.nih.gov/Security/Docs/admin-guide-to-cracking.101.html
CVE-1999-1471	Buffer overflow in passwd in BSD based operating systems 4.3 and earlier allows local users to gain root privileges by specifying a long shell or GECOS field.	http://www.cert.org/advisories/CA-1989-01.html
CVE-1999-1122	Vulnerability in restore in SunOS 4.0.3 and earlier allows local users to gain privileges.	http://www.cert.org/advisories/CA-1989-02.html
CVE-1999-1467	Vulnerability in rcp on SunOS 4.0.x allows remote attackers from trusted hosts to execute arbitrary commands as root, possibly related to the configuration of the nobody user.	http://www.cert.org/advisories/CA-1989-07.html
CVE-1999-1506	Vulnerability in SMI Sendmail 4.0 and earlier, on SunOS up to 4.0.3, allows remote attackers to access user bin.	http://www.cert.org/advisories/CA-90.01.sun.sendmail.vulnerability
CVE-1999-0084	Certain NFS servers allow users to use mknod to gain privileges by creating a writable kmem device and setting the UID to 0.	https://exchange.xforce.ibmcloud.com/vulnerabilities/78
CVE-2000-0388	Buffer overflow in FreeBSD libmytinfo library allows local users to execute commands via a long TERMCAP environmental variable.	ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-00%3A17.libmytinfo.asc
CVE-1999-0209	The SunView (SunTools) selection_svc facility allows remote users to read files.	http://www.securityfocus.com/bid/8
CVE-1999-1198	BuildDisk program on NeXT systems before 2.0 does not prompt users for the root password, which allows local users to gain root privileges.	http://ciac.llnl.gov/ciac/bulletins/b-01.shtml
CVE-2019-15491	openITCOCKPIT before 3.7.1 has CSRF, aka RVID 2-445b21.	https://github.com/it-novum/openITCOCKPIT/releases/tag/openITCOCKPIT-3.7.1

CVE ID	Description	Recommandations
CVE-2008-4242	ProFTPD 1.3.1 interprets long commands from an FTP client as multiple commands, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks and execute arbitrary FTP commands via a long ftp:// URI that leverages an existing session from the FTP client implementation in a web b...	http://bugs.proftpd.org/show_bug.cgi?id=3115
CVE-2001-1422	WinVNC 3.3.3 and earlier generates the same challenge string for multiple connections, which allows remote attackers to bypass VNC authentication by sniffing the challenge and response of other users.	http://www.kb.cert.org/vuls/id/303080
CVE-2002-0971	Vulnerability in VNC, TightVNC, and TridiaVNC allows local users to execute arbitrary code as LocalSystem by using the Win32 Messaging System to bypass the VNC GUI and access the "Add new clients" dialogue box.	http://marc.info/?l=bugtraq&m;=102994289123085&w;=2
CVE-2002-0994	SunPCi II VNC uses a weak authentication scheme, which allows remote attackers to obtain the VNC password by sniffing the random byte challenge, which is used as the key for encrypted communications.	http://archives.neohapsis.com/archives/vulnwatch/2002-q3/0003.html
CVE-2002-1336	TightVNC before 1.2.6 generates the same challenge string for multiple connections, which allows remote attackers to bypass VNC authentication by sniffing the challenge and response of other users.	http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio;=000640
CVE-2002-2088	The MOSIX Project clump/os 5.4 creates a default VNC account without a password, which allows remote attackers to gain root access.	http://archives.neohapsis.com/archives/bugtraq/2002-04/0327.html
CVE-2002-1511	The vncserver wrapper for vnc before 3.3.3r2-21 uses the rand() function instead of srand(), which causes vncserver to generate weak cookies.	http://changelogs.credativ.org/debian/pool/main/v/vnc/vnc_3.3.6-3/changelog
CVE-2006-1652	Multiple buffer overflows in (a) UltraVNC (aka Ultr@VNC) 1.0.1 and earlier and (b) tabbed_viewer 1.29 (1) allow user-assisted remote attackers to execute arbitrary code via a malicious server that sends a long string to a client that connects on TCP port 5900, which triggers an overflow in Log::Real...	http://lists.grok.org.uk/pipermail/full-disclosure/2006-April/044901.html
CVE-2006-4309	VNC server on the AK-Systems Windows Terminal 1.2.5 ExVLP is not password protected, which allows remote attackers to login and view RDP or Citrix sessions.	http://securityreason.com/securityalert/1438
CVE-2007-0756	Chicken of the VNC (cotv) 2.0 allows remote attackers to cause a denial of service (application crash) via a large computer-name size value in a ServerInit packet, which triggers a failed malloc and a resulting NULL dereference.	http://osvdb.org/33637
CVE-2007-0998	The VNC server implementation in QEMU, as used by Xen and possibly other environments, allows local users of a guest operating system to read arbitrary files on the host operating system via unspecified vectors related to QEMU monitor mode, as demonstrated by mapping files to a CDROM device. NOTE: ...	http://fedoranews.org/cms/node/2802
CVE-2000-1169	OpenSSH SSH client before 2.3.0 does not properly disable X11 or agent forwarding, which could allow a malicious SSH server to gain access to the X11 display and sniff X11 events, or gain access to the ssh-agent.	http://archives.neohapsis.com/archives/bugtraq/2000-11/0195.html
CVE-2002-0402	Buffer overflow in X11 dissector in Ethereal 0.9.3 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code while Ethereal is parsing keysyms.	ftp://ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-037.0.txt

CVE ID	Description	Recommandations
CVE-2002-0517	Buffer overflow in X11 library (libX11) on Caldera Open UNIX 8.0.0, UnixWare 7.1.1, and possibly other operating systems, allows local users to gain root privileges via a long -xrm argument to programs such as (1) dtterm or (2) xterm.	ftp://stage.caldera.com/pub/security/openunix/CSSA-2002-SCO.15/CSSA-2002-SCO.15.txt
CVE-2004-0157	x11.c in xonix 1.4 and earlier uses the current working directory to find and execute the rmail program, which allows local users to execute arbitrary code by modifying the path to point to a malicious rmail program.	http://secunia.com/advisories/11382
CVE-2004-2097	Multiple scripts on SuSE Linux 9.0 allow local users to overwrite arbitrary files via a symlink attack on (1) /tmp/fvwm-bug created by fvwm-bug, (2) /tmp/wmmenu created by wm-oldmenu2new, (3) /tmp/rates created by x11perfcomp, (4) /tmp/xf86debug.1.log created by xf86debug, (5) /tmp/.winpopup-new cre...	http://marc.info/?l=bugtraq&m;=107461582413923&w;=2
CVE-2005-0084	Buffer overflow in the X11 dissector in Ethereal 0.8.10 through 0.10.8 allows remote attackers to execute arbitrary code via a crafted packet.	http://secunia.com/advisories/13946/
CVE-2005-3248	Unspecified vulnerability in the X11 dissector in Ethereal 0.10.12 and earlier allows remote attackers to cause a denial of service (divide-by-zero) via unknown vectors.	http://secunia.com/advisories/17254
CVE-2006-0577	Lexmark X1185 printer allows local users to gain SYSTEM privileges by navigating to the "Appearance" dialog and selecting the "Additional styles (skins) are available on the Lexmark web site" option, which launches a web browser that is running with SYSTEM privileges.	http://secunia.com/advisories/18728
CVE-2006-0745	X.Org server (xorg-server) 1.0.0 and later, X11R6.9.0, and X11R7.0 inadvertently treats the address of the geteuid function as if it is the return value of a call to geteuid, which allows local users to bypass intended restrictions and (1) execute arbitrary code via the -modulepath command line opti...	http://secunia.com/advisories/19256
CVE-2006-3470	The Dell Openmanage CD launches X11 and SSH daemons that do not require authentication, which allows remote attackers to gain privileges.	http://msgs.securepoint.com/cgi-bin/get/bugtraq0606/187.html
CVE-2004-0679	The IP cloaking feature (cloak.c) in UnrealIRCd 3.2, and possibly other versions, uses a weak hashing scheme to hide IP addresses, which could allow remote attackers to use brute force methods to gain other user's IP addresses.	http://marc.info/?l=bugtraq&m;=108904813003166&w;=2
CVE-2006-1214	UnrealIRCd 3.2.3 allows remote attackers to cause an unspecified denial of service by causing a linked server to send malformed TKL Q:Line commands, as demonstrated by "TKL - q\x08Q *\x08PoC."	http://forums.unrealircd.com/viewtopic.php?t=2985
CVE-2009-4893	Buffer overflow in UnrealIRCd 3.2beta11 through 3.2.8, when allow::options::noident is enabled, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors.	http://security.gentoo.org/glsa/glsa-201006-21.xml
CVE-2010-2075	UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally introduced modification (Trojan Horse) in the DEBUG3_DOLOG_SYSTEM macro, which allows remote attackers to execute arbitrary commands.	http://osvdb.org/65445
CVE-2013-6413	Use-after-free vulnerability in UnrealIRCd 3.2.10 before 3.2.10.2 allows remote attackers to cause a denial of service (crash) via unspecified vectors. NOTE: this identifier was SPLIT per ADT2 due to different vulnerability types. CVE-2013-7384 was assigned for the NULL pointer dereference.	http://forums.unrealircd.com/viewtopic.php?f=2&t;=8221

CVE ID	Description	Recommandations
CVE-2013-7384	UnrealIRCd 3.2.10 before 3.2.10.2 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via unspecified vectors, related to SSL. NOTE: this issue was SPLIT from CVE-2013-6413 per ADT2 due to different vulnerability types.	http://forums.unrealircd.com/viewtopic.php?f=2&t;=8221
CVE-2016-7144	The m_authenticate function in modules/m_sasl.c in UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6 allows remote attackers to spoof certificate fingerprints and consequently log in as another user via a crafted AUTHENTICATE parameter.	http://www.openwall.com/lists/oss-security/2016/09/04/3
CVE-2017-13649	UnrealIRCd 4.0.13 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command. NOTE: th...	http://www.securityfocus.com/bid/100507
CVE-2023-50784	A buffer overflow in websockets in UnrealIRCd 6.1.0 through 6.1.3 before 6.1.4 allows an unauthenticated remote attacker to crash the server by sending an oversized packet (if a websocket port is open). Remote code execution might be possible on some uncommon, older platforms.	https://forums.unrealircd.org/viewtopic.php?t=9340
CVE-2000-1247	The default configuration of the jserv-status handler in jserv.conf in Apache JServ 1.1.2 includes an "allow from 127.0.0.1" line, which allows local users to discover JDBC passwords or other sensitive information via a direct request to the jserv/ URI.	http://archive.apache.org/dist/java/java.apache.org-www.tar.gz
CVE-2020-1938	When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that ...	http://lists.opensuse.org/opensuse-security-announce/2020-03/msg00025.html

Résultats de l'attaque par dictionnaire Hydra:

Les résultats ci-dessous montrent les tentatives d'attaque par dictionnaire réussies. Veuillez vérifier les informations et prendre les mesures nécessaires pour sécuriser les services.

Utilisateur	Mot de passe	Heure	Type
msfadmin	msfadmin	2024-06-27 20:22:30	SSH

Conclusion:

Le présent rapport a permis de mettre en lumière plusieurs vulnérabilités présentes dans les services et versions détectés sur les hôtes analysés. Les CVE identifiées montrent une gamme de risques potentiels qui doivent être traités pour améliorer la sécurité globale de l'infrastructure.

Principales recommandations :
1. **Mises à jour et correctifs** : Assurez-vous que tous les logiciels et services sont à jour avec les derniers correctifs de sécurité. Les versions obsolètes des services sont souvent les plus vulnérables

aux attaques.
2. **Renforcement des configurations** : Appliquez des configurations de sécurité renforcées pour les services critiques. Désactivez les services non utilisés pour réduire la surface d'attaque.
3. **Surveillance continue** : Mettez en place des systèmes de surveillance pour détecter et alerter rapidement en cas d'activités suspectes. Une surveillance proactive peut aider à prévenir les incidents de sécurité.
4. **Audits réguliers** : Effectuez des audits de sécurité réguliers pour identifier et corriger les nouvelles vulnérabilités. Les audits fréquents permettent de maintenir un haut niveau de sécurité.
5. **Formation et sensibilisation** : Assurez-vous que le personnel est formé et conscient des meilleures pratiques en matière de sécurité informatique. Une formation adéquate peut réduire les erreurs humaines qui sont souvent à l'origine des incidents de sécurité.

En suivant ces recommandations et en traitant les vulnérabilités identifiées dans ce rapport, vous pouvez améliorer considérablement la posture de sécurité de votre organisation. Une attention continue à la sécurité et une mise en œuvre diligente des correctifs et des améliorations sont essentielles pour protéger vos actifs numériques contre les menaces en constante évolution. Pour toute question ou assistance supplémentaire, n'hésitez pas à contacter notre équipe de sécurité.