



QUANTUM

04 July 2024

GAIA

R80.40

Hardening Specifications



Check Point Copyright Notice

© 2020 - 2024 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the [Copyright page](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.

Important Information



Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



Certifications

For third party independent certification of Check Point products, see the [Check Point Certifications page](#).



Check Point R80.40

For more about this release, see the R80.40 [home page](#).



Latest Version of this Document in English

Open the latest version of this [document in a Web browser](#).
Download the latest version of this [document in PDF format](#).



Feedback

Check Point is engaged in a continuous effort to improve its documentation. [Please help us by sending your comments](#).

Revision History

Date	Description
22 June 2022	In the HTML version, added glossary terms in the text
01 March 2021	First release of this document

Table of Contents

Gaia Hardening	6
Important Notes	6
Network Services Supported in Gaia	7
Restricted Shell in Gaia	8
Kernel Changes	9
Unchanged RPM Packages from RHEL 7.x / 8	10
Modified RPM Packages from RHEL 7.x / 8	14
Unchanged RPM Packages from RHEL 5.2	15
Modified RPM Packages from RHEL 5.2	18

Gaia Hardening

This document describes the hardening of the Check Point Gaia operating system.

Components that are not necessary for a network security device, or that could cause security vulnerabilities, were removed.

Check Point Gaia R80.40 is based on Red Hat 7.6 version and the Linux kernel 3.10.0-957.

The applications removed from the operating system include X Windows, Office applications, games, and many other applications that are irrelevant to Firewall operations.

This document describes the remaining packages and modifications to the system.

Important Notes


- RPMs not needed for network security services were removed.
- The RPMs listed in this document refer to Check Point Gaia R80.40 version.
- The list of RPMs does not include Check Point application packages that are installed on the Gaia system. The list only applies to the Gaia operating system hardening.
- Gaia OS is derived from a Red Hat Linux distribution. The source code for these modified packages is available for review, as described in the **License.txt** file on the Gaia distribution media.
- The hardening of some Gaia components, such as those requiring external network communications, was audited by Check Point staff and by an independent security consulting organization.

Network Services Supported in Gaia

After Gaia OS is installed, the only network services on Gaia OS are:

Service	Description
OpenSSH	Used for remote console login. Listens on the TCP port 22.
Check Point secure web server	Used for system administration using a Web user interface. Access is over HTTPS. Listens on the TCP port 443.
Check Point remote installation daemon 'cprid'	Used for Check Point software management. Listens on the TCP port 18208.
Check Point Secure REST API Server	Used for system administration over HTTPS. Listens on the TCP port 443 (proxy through a web server).

After the Check Point applications are enabled, several more processes listen to the network traffic. These processes are all used by the different Management, Firewall, and VPN operations to perform Check Point Secure Internal Communication (SIC).

-  **Note** - The Check Point secure web server was developed internally at Check Point. It is based on the industry standard Apache Web Server, hardened, and configured to show only the Gaia Portal.

Restricted Shell in Gaia

A Gaia device is usually managed using a restricted shell.

- Only the utilities needed to manage Check Point products are allowed.

These utilities were wrapped with code to disable some of the options that are not necessary.

The utilities are made simpler for customer use.

- No special characters are supported - only letters, numbers, space, and tab are supported. Piping is disabled.
- "Expert" mode, which requires an additional password, provides access to the regular Linux shell (Bash).

Kernel Changes

- Fixed SKB memory leaks.
- Made SKB memory optimizations.
- Added patches for newer `ixgbe` and `e1000e` drivers.
- Added the ENA driver.
- Packet-per-Second (pps) optimization when GRO is disabled.
- Modified the kernel configuration file for performance issues.
- Added support for zeco (zero-copy) packets for Check Point USFW (Firewall in usermode).
- Enabled cluster in Bridge mode to work in the High Availability mode.
- Fixed a vulnerability in SCTP protocol (CVE).
- Fixed kernel vulnerabilities in the TCP SACK PANIC (CVE).
- Changed the kernel image size.
- Added support for Docker.
- Removed the open-coded `'skb_cow_head()'` function.
- Reduced the noise in the `'skb_warn_bad_offload()'` function based on the upstream kernel.
- Added the Bypass driver for Bypass card support.
- Applied errata for the `ixgbe` driver.
- Added support to new line of Check Point appliances.
- Moved the errata `'TSC_DEADLINE'` information from console to `dmesg`.
- Modified the `'set_irq_affinty'` function in the `i40e` driver for better support of Check Point Multi-Queue.
- Removed the KABYLAKE CPU warning (because it is supported).
- Changed the accounting `CONFIG_IRQ_TIME_ACCOUNTING`.

Unchanged RPM Packages from RHEL 7.x / 8

The RPM packages listed below were imported with several changes from RHEL 7.4/7.6 distribution.

Check Point removed the manual files (man pages) and the language localization files.

List of unchanged RPM packages:

1. `acpid`
2. `attr`
3. `audit-rhel-libs`
4. `bash`
5. `chkconfig`
6. `containers-common`
7. `coreutils`
8. `device-mapper`
9. `device-mapper-event`
10. `device-mapper-eventlibs`
11. `device-mapper-libs`
12. `dmidecode`
13. `dmraid`
14. `dmraid-events`
15. `docker-client`
16. `docker-common`
17. `dos2unix`
18. `e2fsprogs`
19. `elfutils-libs`
20. `ethtool`
21. `filesystem`
22. `gawk`

23. gdisk
24. glibc
25. glibc-2
26. glibc-common
27. gpgme
28. grep
29. gzip
30. hdparm
31. htop
32. hwdata
33. ibassuan
34. iotop
35. iproute
36. krb5-libs
37. libattr
38. libblkid
39. libcom_err
40. libdb
41. libdb-utils
42. libdnf
43. libffi
44. libgcc
45. libgpg-error
46. libmount
47. libmspack
48. libn13
49. libpcap
50. libseccomp
51. libselinux

52. libss
53. libstdc++
54. libsysfs
55. libtirpc
56. libusb
57. libusbx
58. libuser
59. libuuid
60. lm_sensors
61. lm_sensors-libs
62. lsscsi
63. lvm2-libs
64. lvm2-sysvinit
65. mcstrans
66. mdadm
67. ncurses
68. ncurses-base
69. ncurses-libs
70. ncurses-term
71. nfs-utils
72. nspr
73. nss
74. nss-pem
75. nss-softokn
76. nss-softokn-freebl
77. nss-sysinit
78. nss-util
79. ntp
80. numactl

81. numactl-libs
82. openssh (based on RedHat 8)
83. open-vm-tools
84. parted
85. pciutils
86. pciutils-libs
87. pcre
88. pcre-tools
89. procps-ng
90. psmisc
91. rsync
92. sed
93. sudo
94. sysfsutils
95. sysstat
96. sysvinit-tools
97. tar
98. tcpdump
99. tcsh
100. tftp
101. tftp-server
102. tzdata-2018g
103. usbutils
104. usermode
105. util-linux
106. virt-what
107. which
108. xfsdump
109. xfsprogs

Modified RPM Packages from RHEL 7.x / 8

Check Point modified the RPM packages listed below that are part of the RHEL 7.4/7.6 distribution.

Check Point removed the manual files (man pages) and the language localization files.

List of modified RPM packages:

#	RPM	Changes
1	cifs-utils	Removed the default 'dns_resolver' because Check Point uses the 'cifs.upcall dns_resolver'.
2	docker	Adaption for Check Point software.
3	lvm2	Added a 64-bit flavor.
4	net-snmp	Added SHA-256 and SHA-512 support for USM users.

Unchanged RPM Packages from RHEL 5.2

The RPM packages listed below were imported with several changes from RHEL 5.2 distribution.

Check Point removed the manual files (man pages) and the language localization files.

List of unchanged RPM packages:

1. audit
2. basesystem
3. beecrypt
4. bridge-utils
5. busybox
6. bzip2
7. cpio
8. device-mapper-multipath
9. dhclient
10. dhcp
11. diffutils
12. dnsmasq
13. dump
14. expat
15. file
16. findutils
17. gnome-libs
18. hping
19. iputils
20. kbd
21. less
22. libacl

23. libcap
24. libelf-utils
25. libnl
26. libsepol
27. libtermcap
28. libxml2
29. libxslt
30. lsof
31. mktemp
32. mount (comes with util-linux rpm)
33. msmtpt
34. mtools
35. mt-st
36. nash
37. netcat
38. OpenIPMI
39. os_syslinux
40. os_udevtool
41. os_webTerminal
42. passwd
43. popt
44. procps
45. rarpd
46. readahead
47. readline
48. rootfiles
49. samba-client
50. sqlite
51. squashfs-tools

52. SysVinit
53. tcp_wrappers
54. termcap
55. traceroute
56. udev
57. vconfig

Modified RPM Packages from RHEL 5.2

Check Point modified the RPM packages listed below that are part of the RHEL 5.2 distribution.

Check Point removed the manual files (man pages) and the language localization files.

List of modified RPM packages:

#	RPM	Changes
1	bind-utils	The 'libs' package is not installed. The Development SDK is not installed. Added fixes for several CVEs from RHEL 5.11 distribution.
2	cracklib	Fixed a "password" bug.
3	db1	Required by RPM. The Development SDK is not installed.
4	ftp:(ftp client)	Passive FTP client ('pftp') is not installed.
5	gdbm	Required by RPM. The Development SDK is not installed.
6	glib	Only the necessary component ('libglib') is installed. The Development SDK is not installed.
7	grub	Changes for an automatic serial console support. Some GUI changes. Added a patch to support SHA-2. Added a patch for performance enhancement.
8	initscripts	"Pretty" boot with progress dots on the VGA console (no graphical boot). Removed the Red Hat network configuration scripts. A different shell reads a password. Added a control for the LED to show the machine state. Configures the Logical Volume Management (LVM2) at startup.

#	RPM	Changes
9	kudzu	Fixed bugs with installation and configuration on some devices (SCSI bus crash, network interfaces recognition, Adaptec NIC configuration, and other bugs). Fixed bugs related to Ethernet number for NIC. Fixed bugs related to interface names. Added support for VirtIO disk driver.
10	linux-firmware	Added the 'esp-ah.pkg' for the i40e driver.
11	MAKEDEV	Changes to contain only supported devices in /dev/ (no entries for graphical cards, sound cards, mouse, and so on).
12	microcode_ctl	Removed the 'modeprobe' of the microcode (because it is built-in into the kernel).
13	mkinitrd	Support for Check Point boot menu. Root device on an LVM volume is handled directly from 'nash'. Removed the 'strip' command, which does not support the 64-bit *.ko files.
14	ncusers	Reduced the size of the 'terminfo' database to several useful entries. The development components are not installed.
15	net-tools	Fixed bugs related to configuration of netmask and of NIC states.
16	openlldp	Fixed bugs related to memory allocation. Fixed bugs that cause crashes.
17	openssl	Check Point packages only the 'libcrypto' because it is required for SSH. Kerberos is not packaged. No compilation of the OpenSSL thread test. Fixed the Oracle Timing/Side Channel padding vulnerability
18	ppp	Fixed CVE-2020-8597 (a buffer overflow vulnerability).

#	RPM	Changes
18	pam	Use Check Point MD5 function to avoid a blow up caused by OS secret MD5 library functions. Included RADIUS (Remote Authentication Dial In User Service). Included PAM to RADIUS authentication module. Added RADIUS groups. Add the sha2 patch.
19	pptp-client	Not a Red Hat RPM. Imported from the Mandrake Linux.
20	rp-pppoe	Removed configuration settings.
21	rpm	Excluded the 'libs' package that contains RPM shared libraries. Added the POPT Development SDK. If Python can use the RPM libraries, the POSIX Mutexes are disabled. Excluded the RPM build package. Patch to enable installation of 32-bit and 64-bit RPMs. Output enhancement to show the CPU architecture.
22	setup	Removed some user accounts from the <code>/etc/passwd</code> and <code>/etc/groups</code> files. Log out the user after three minutes of unattended prompt (in Bash). Generation of core dump files is enabled by default. Added aliases for the 'll' and 'take.info' commands.
23	shadow-utils	Added a patch to support a period "." character in a user/group name.
24	sharutils	Includes only the 'uuencode' and 'uudecode'.
25	sysklogd	Excluded the syslog 'local5' facility.
26	telnet	The telnet server is installed by default. If the telnet server is installed, then it is disabled by default.
27	Vi	Included the 'nvi' editor (as an alternative to a much larger 'vim').
28	vixiecron	Uses the 'logger' as an alternative to sending a mail.
29	xinetd	No services by default.

#	RPM	Changes
30	zlib	No services by default.