ASSURANCE CONTINUITY MAINTENANCE REPORT FOR RED HAT ENTERPRISE LINUX 9.0 EUS

Maintenance Update of Red Hat Enterprise Linux 9.0 EUS

Maintenance Report Number: CCEVS-VR-VID11379-2024

Date of Activity: 9 September 2024

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016;

Red Hat Enterprise Linux 9.0 EUS

Impact Analysis Report, Version 0.7, August 2024

Documentation Updated: The original documentation has been updated to the following:

Security Target: Red Hat Enterprise Linux 9.0 EUS Security Target, Version 2.1, August 2024. Changes in the Security Target are:

- TOE version updated to Red Hat Enterprise Linux 9.0 EUS cc-config-9.0-2.
- Security Target updated to Red Hat Enterprise Linux 9.0 EUS Security Target, Version 2.1, August 2024.
- AGD reference updated to Red Hat Enterprise Linux 9.0 EUS Common Criteria Guide, Version 2.1, August 2024
- Correction of hardware platform specification for IBM z16 and Power10 PowerVM platforms.

Guidance Documentation: Changes were made to the guidance documentation, including:

- TOE version updated to Red Hat Enterprise Linux 9.0 EUS cc-config-9.0-2.
- Details for downloading the updated TOE version.
- AVA updated to include the vulnerability mitigation details of 5 CVEs previously left unmitigated
- Correction of hardware platform specification for IBM z16 and Power10 PowerVM platforms.

- AGD updated to add the uio module to the denylist
- IAR updated regarding the uio module denylist

Assurance Continuity Maintenance Report:
Red Hat, Inc. submitted an Impact Analysis Report (IAR) and Assurance Continuity Maintenance package to the CCEVS for approval in March 2024. There were some discrepancies in CVE mitigations as part of that package in Mid-May. Subsequently the lab had to address mitigations of 5 of those tyes of CVEs and submitted an updated package in August 2024. The IAR is intended to satisfy the requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the validated TOE, the evidence updated because of the changes, and the security impact of the changes.

The updated public vulnerability search was performed on May 28, 2024. All potential vulnerabilities were determined to be mitigated/fixed or not applicable to the evaluated configuration. No residual vulnerabilities were identified.

Changes to TOE:
Red Hat, Inc. made changes to the Kernel, OpenSSL, and the TOE configuration to address vulnerabilities and fix bugs discovered in the validated TOE. The TOE was updated through several kernel updates (kernel-5.14.0-70.85.1.el9_0, kernel-5.14.0-70.88.1.el9_0, and kernel-5.14.0-70.93.2.el9_0), listed in the following tables:

kernel-5.14.0-70.85.1.el9_0 Changes	
Change	**Analysis**
kernel: xfrm_expand_policies() in net/xfrm/xfrm_policy.c can cause a refcount to be dropped twice (CVE-2022-36879)	Minor: No evaluated functionality uses xfrm. This is unevaluated functionality that is not touched in any way by the CC testing or SFRs.
kernel: null-ptr-deref vulnerabilities in sl_tx_timeout in drivers/net/slip (CVE-2022-41858)	Minor: The evaluated configuration prevents loading of the module containing the flaw; therefore, this change has no impact on the operation of the TOE.
kernel: use-after-free caused by invalid pointer hostname in fs/cifs/connect.c (CVE-2023-1195)	Minor: No evaluated functionality uses cifs. This is unevaluated functionality that is not touched in any way by the CC testing or SFRs.
kernel: UAF during login when accessing the shost ipaddress (CVE-2023-2162)	Minor: The evaluated configuration prevents loading of the module containing the flaw and fix; therefore,

kernel-5.14.0-70.85.1.el9_0 Changes	
Change	**Analysis**
	this change has no impact on the operation of the TOE.
kernel: use after free in vcs_read in drivers/tty/vt/vc_screen.c due to race (CVE-2023-3567)	Minor: This is related to TTY functionality. This update does not change the TTY functionality associated with the local console, only patches the vulnerability.
kernel: use-after-free in netfilter: nf_tables (CVE-2023-3777)	Minor: This is a fix to memory/list management. It does not change the firewall functionality.
kernel: net/sched: sch_hfsc UAF (CVE-2023-4623)	Minor: The evaluated configuration prevents loading of the module containing the flaw and fix; therefore, this change has no impact on the operation of the TOE.
kernel: use after free in nvmet_tcp_free_crypto in NVMe (CVE-2023-5178)	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
kernel: IGB driver inadequate buffer size for frames larger than MTU (CVE-2023-45871)	Minor: This is a small additional check to compare the buffer size to the MTU.
kernel: SEV-ES local priv escalation (CVE-2023-46813)	Minor: No evaluated functionality uses SEV-ES. This is unevaluated functionality that is not touched in any way by the CC testing or SFRs.
RHEL 9 Hyper-V: Excessive hv_storvsc driver logging with srb_status SRB_STATUS_INTERNAL_ERROR (0x30)	Minor: No evaluated platforms test the TOE on Hyper-V. This does not have any impact on the evaluated platforms.
RHEL9.0 - s390/qeth: NET2016 - fix use-after-free in HSCI DM multipath showing failed path for an nvme-o-FC LUN when performing I/O operations	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an

kernel-5.14.0-70.85.1.el9_0 Changes	
Change	**Analysis**
	adverse impact.
XFS: sync to upstream v5.15 AMDSERVER 9.4 Bug, Turin: Support larger microcode patches	Minor: No evaluated platforms test the TOE on AMD processors. This does not have any impact on the evaluated platforms.

kernel-5.14.0-70.88.1.el9_0 Changes	
Change	**Analysis**
CVE-2023-38409 kernel: fbcon: out-of-sync arrays in fbcon_mode_deleted due to wrong con2fb_map assignment	Minor: The evaluated configuration prevents loading of the module containing the flaw and fix; therefore, this change has no impact on the operation of the TOE.
[SanityOnly][kernel]BUG: sleeping function called from invalid context at kernel/locking/spinlock_rt.c:35 at: sock_map_update_elem_sys+0x85/0x2a0	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
CVE-2023-4459 kernel: vmxnet3: NULL pointer dereference in vmxnet3_rq_cleanup()	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
CVE-2023-2166 kernel: NULL pointer dereference in can_rcv_filter	Minor: The evaluated configuration prevents loading of the module containing the flaw and fix; therefore, this change has no impact on the operation of the TOE.
CVE-2022-40982 kernel: hw: Intel: Gather Data Sampling (GDS) side channel vulnerability	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing

kernel-5.14.0-70.88.1.el9_0 Changes	
Change	**Analysis**
	shows the change does not have an adverse impact.
CVE-2023-5717 kernel: A heap out-of-bounds write	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
CVE-2023-2176 kernel: Slab-out-of-bound read in compare_netdev_and_ip	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
CVE-2022-3545 kernel: A flaw leading to a use-after-free in area_cache_get()	Minor: No evaluated platforms test the TOE with hardware that would load the vulnerable driver. This does not have any impact on the evaluated platforms.
CVE-2023-2163 kernel: bpf: Incorrect verifier pruning leads to unsafe code paths being incorrectly marked as safe	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
CVE-2023-1192 kernel: use-after-free in smb2_is_status_io_timeout()	Minor: The evaluated configuration prevents loading of the module containing the flaw and fix; therefore, this change has no impact on the operation of the TOE.
CVE-2023-4622 kernel: various flaws	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
CVE-2023-40283 kernel: use-after-free in	Minor: No evaluated platforms test the

kernel-5.14.0-70.88.1.el9_0 Changes	
Change	**Analysis**
l2cap_sock_release in net/bluetooth/l2cap_sock.c	TOE with hardware that would load the vulnerable driver. This does not have any impact on the evaluated platforms.
CVE-2023-7192 kernel: refcount leak in ctnetlink_create_conntrack()	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
RHEL9.0 - s390/qeth: recovery and set offline lose routes and IPv6 addr	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
CVE-2023-3609 kernel: net/sched: cls_u32 component reference counter leak if tcf_change_indev() fails	Minor: The evaluated configuration prevents loading of the module containing the flaw and fix; therefore, this change has no impact on the operation of the TOE.
CVE-2023-3268 kernel: out-of-bounds access in relay_file_read	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.

kernel-5.14.0-70.93.2.el9_0 Changes	
Change	**Analysis**
RHEL-9.0 TEST-17-Setup-struct-perf-event-attr / bz1308907 test failure on Ice Lake	Minor: No evaluated platforms test the TOE on Ice Lake processors. This does not have any impact on the evaluated platforms.
dm multipath device suspend deadlocks waiting on a	Minor: This is a small change in low

kernel-5.14.0-70.93.2.el9_0 Changes	
Change	**Analysis**
flush request	level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
Unbounded memory usage by TCP for receive buffers	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
CVE-2023-6932 kernel: use-after-free in IPv4 IGMP	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
CVE-2024-0646 kernel: ktls overwrites readonly memory pages when using function splice with a ktls socket as destination	Minor: The evaluated configuration prevents loading of the module containing the flaw and fix; therefore, this change has no impact on the operation of the TOE.
5.14.0-70.87.1.el9_0: aarch64 BUG: arch topology borken / the CLS domain not a subset of the MC domain	Minor: No evaluated platforms test the TOE on aarch64 processors. This does not have any impact on the evaluated platforms.
kernel: UAF in nftables when nft_set_lookup_global triggered after handling named and anonymous sets in batch requests (CVE-2023-3390)	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
kernel: Race Condition leading to UAF in Unix Socket could happen in sk_receive_queue ()	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an

kernel-5.14.0-70.93.2.el9_0 Changes	
Change	**Analysis**
	adverse impact.
rbd: don't move requests to the running list on errors (JIRA:RHEL-23861)	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
kernel: memcg does not limit the number of POSIX file locks allowing memory exhaustion (CVE-2022-0480)	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
kernel: GSM multiplexing race condition leads to privilege escalation (CVE-2023-6546)	Minor: The evaluated configuration prevents loading of the module containing the flaw and fix; therefore, this change has no impact on the operation of the TOE.
kernel: vmxgfx: NULL pointer dereference in vmw_cmd_dx_define_query (CVE-2022-38096)	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.
kernel: sched/membarrier: reduce the ability to hammer on sys_membarrier (CVE-2024-26602)	Minor: This is a small change in low level functionality that supports but is not directly related to evaluated functionality. The Regression Testing shows the change does not have an adverse impact.

OpenSSL was updated to openssl-3.0.1-46.el9_0.4. The following table summarizes changes to OpenSSL:

OpenSSL Changes

Change	Analysis
CVE-2023-2650 openssl: Possible DoS translating ASN.1 object identifiers [rhel-9.0.0.z] (RHEL-5315)	Minor: This bug fix affects the ASN.1 parser that is used in OCSP. This does not affect OCSP itself, so it is considered a minor change. Additionally, the OCSP functionality was independently retested by the testing lab that conducted the original product evaluation after regression testing by Red Hat, Inc.

The TOE was updated to mitigate exploitation of several kernel vulnerabilities by adding the affected kernel modules to a denylist. The following table summarizes configuration changes made to the TOE.

OS Configuration Changes	
Change	**Analysis**
Add Kernel module n_gsm to the denylist to prevent it from being loaded.	Minor: The evaluated confirmation and functionality do not use the n_gms kernel module. Adding it to the denylist ensures it cannot be loaded and exploited.
Add Kernel module tls to the denylist to prevent it from being loaded.	Minor: The evaluated confirmation and functionality do not use the tls kernel module. Adding it to the denylist ensures it cannot be loaded and exploited.
Add Kernel module drm to the denylist to prevent it from being loaded.	Minor: The evaluated confirmation and functionality do not use the drm kernel module. Adding it to the denylist ensures it cannot be loaded and exploited.
Add Kernel module raid5 to the denylist to prevent it from being loaded.	Minor: The evaluated confirmation and functionality do not use the raid5 kernel module. Adding it to the denylist ensures it cannot be loaded and exploited.
Add Kernel module cec to the denylist to prevent it from being loaded.	Minor: The evaluated confirmation and functionality do not use the cec kernel module. Adding it to the denylist ensures it cannot be loaded and exploited.

Below is a summary of all the above changes, in terms of source/type of change, number of changes and their impact analysis rationale. Note that all the changes had minor security impact on the TOE.

Source/Type of Changes	# of Changes	Impact analysis rationale summary
kernel-5.14.0-70.85.1.el9_0 Changes	13	The corresponding kernel changes affected modules, which are either not part of the evaluated configuration, or not loaded, or not part of evaluated platform, or not directly related to evaluated functionality
kernel-5.14.0-70.88.1.el9_0 Changes	16	Most of the changes are not directly related to evaluated functionality, some other are either outside evaluated functionality or unloaded functionality
kernel-5.14.0-70.93.2.el9_0 Changes	13	Most of the changes are not directly related to evaluated functionality, some other are outside evaluated functionality or unloaded functionality
OpenSSL Changes	1	Bug fixes in a parser in OCSP that doesn't affect the OCSP itself
OS Configuration Changes	5	affected kernel modules are added to the denylist

Equivalency Discussion:

Red Hat, Inc. initiated this maintenance action to address residual vulnerabilities present in the TOE at the time its evaluation completed. Red Hat patched the vulnerable components, integrated the patches into the TOE, and developed and executed testing activities to determine whether the issues identified in their vulnerability analysis had been corrected. Red Hat also performed regression testing of the entire TOE to ensure that the TOE continued to perform as expected at the time of the original evaluation. Finally, the independent test laboratory that conducted the initial TOE evaluation formulated and executed regression tests to ensure that the vulnerabilities identified were mitigated, that no new vulnerabilities were introduced into the relevant components, and that the assurance of the evaluated functionality was maintained.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found the changes to be minor and did not affect the evaluated security functionality. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.