

[Red Hat Product Errata](#) [RHSA-2025:15828 - Security Advisory](#)

RHSA-2025:15828 - Security Advisory

Issued: 2025-09-15

Updated: 2025-09-15

[Overview](#)[Updated Images](#)

Synopsis

Important: updated web-terminal/tooling container image

Type/Severity

Security Advisory: Important

Topic

Updated web-terminal/tooling container image is now available for Red Hat Web Terminal 1.11 on RHEL 9.

Description

The Red Hat Web Terminal 1.11 on RHEL 9 container images have been updated to fix the following important CVEs: CVE-2025-5914, CVE-2025-49794, CVE-2025-49796, CVE-2025-6020, CVE-2025-48384, CVE-2025-48385, CVE-2025-7425, CVE-2025-6965, CVE-2025-8941.

Users of Red Hat Web Terminal 1.11 on RHEL 9 container images are advised to upgrade to these updated images, which contain backported patches to correct these security issues, fix these bugs and add these enhancements. Users of these images are also encouraged to rebuild all container images that depend on these images.

You can find images updated by this advisory in Red Hat Container Catalog (see References).

Solution










The Red Hat Web Terminal 1.11 on RHEL 9 container images provided by this update can be downloaded from the Red Hat Container Registry at registry.access.redhat.com. Installation instructions for your platform are available at Red Hat Container Catalog (see References).

Dockerfiles and scripts should be amended either to refer to this new image specifically, or to the latest image generally.

Affected Products

- Red Hat Web Terminal Container Advisories x86_64

Fixes

- [BZ - 2370861](#)  - CVE-2025-5914 libarchive: Double free at archive_read_format_rar_seek_data() in archive_read_support_format_rar.c
- [BZ - 2372373](#)  - CVE-2025-49794 libxml: Heap use after free (UAF) leads to Denial of service (DoS)
- [BZ - 2372385](#)  - CVE-2025-49796 libxml: Type confusion leads to Denial of service (DoS)
- [BZ - 2372512](#)  - CVE-2025-6020 linux-pam: Linux-pam directory Traversal
- [BZ - 2378806](#)  - CVE-2025-48384 git: Git arbitrary code execution
- [BZ - 2378808](#)  - CVE-2025-48385 git: Git arbitrary file writes
- [BZ - 2379274](#)  - CVE-2025-7425 libxslt: Heap Use-After-Free in libxslt caused by atype corruption in xmlAttrPtr
- [BZ - 2380149](#)  - CVE-2025-6965 sqlite: Integer Truncation in SQLite
- [BZ - 2388220](#)  - CVE-2025-8941 linux-pam: Incomplete fix for CVE-2025-6020

CVEs

- [CVE-2019-12900](#) 
- [CVE-2020-11023](#) 
- [CVE-2022-29458](#) 
- [CVE-2023-4752](#) 
- [CVE-2023-45288](#) 
- [CVE-2024-8176](#) 
- [CVE-2024-12133](#) 
- [CVE-2024-12243](#) 
- [CVE-2024-12797](#) 
- [CVE-2024-23337](#) 
- [CVE-2024-50349](#) 
- [CVE-2024-52006](#) 
- [CVE-2024-52533](#) 
- [CVE-2024-53920](#) 

- [CVE-2025-3576](#)
- [CVE-2025-4373](#)
- [CVE-2025-5914](#)
- [CVE-2025-6020](#)
- [CVE-2025-6965](#)
- [CVE-2025-7425](#)
- [CVE-2025-8058](#)
- [CVE-2025-8941](#)
- [CVE-2025-22871](#)
- [CVE-2025-26465](#)
- [CVE-2025-27613](#)
- [CVE-2025-27614](#)
- [CVE-2025-32414](#)
- [CVE-2025-32415](#)
- [CVE-2025-40909](#)
- [CVE-2025-46835](#)
- [CVE-2025-48060](#)
- [CVE-2025-48384](#)
- [CVE-2025-48385](#)
- [CVE-2025-49794](#)
- [CVE-2025-49796](#)

References

- <https://access.redhat.com/security/updates/classification/#important>
- <https://catalog.redhat.com/software/containers/registry/registry.access.redhat.com/repository/web-terminal/tooling>

The Red Hat security contact is secalert@redhat.com. More contact details at <https://access.redhat.com/security/team/contact/>.



